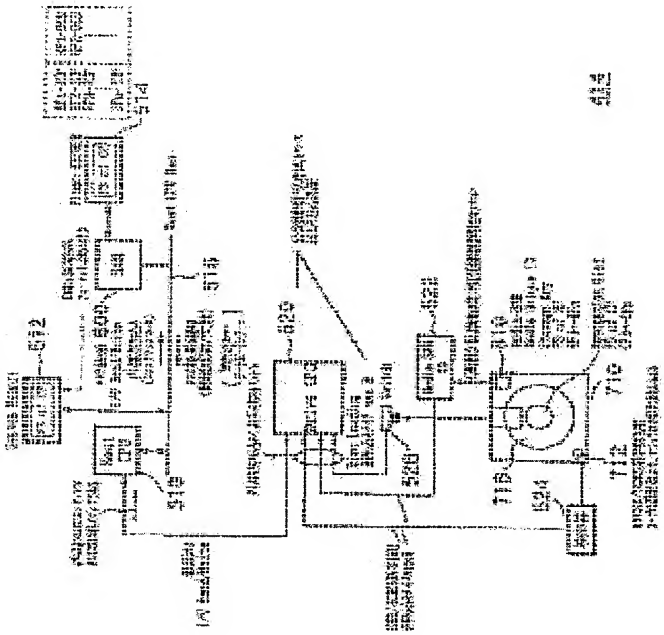
DATA RECORDING DEVICE, DATA REPRODUCING DEVICE, DATA PROCESSING DEVICE AND DATA RECORDING MEDIUM

Publication number: JP2001332023 (A)
Publication date: 2001-11-30
Inventor(s): NONAKA SATOSHI; EZAKI TADASHI +
Applicant(s): SONY CORP +
Classification:
- international: ***G06F12/14; G06F21/24; G10K15/02; G11B19/02; G11B20/10;*** **G06F12/14; G06F21/00; G10K15/02; G11B19/02; G11B20/10;** (IPC1-7): G11B19/02; G11B20/10
- European:
Application number: JP20000152788 20000519
Priority number(s): JP20000152788 20000519

Abstract of **JP 2001332023 (A)**

PROBLEM TO BE SOLVED: To provide a recording device which records and reproduces data while adequately performing right processing and, a reproducing device, a data processing device for delivering the data and a recording medium. SOLUTION: The data is encrypted and delivered and is subjected to the right processing by the secure processing means mounted at respective apparatus. The data is recorded and reproduced only in the case of the adequate right. The secure processing means having key data, authentication means, etc., are mounted at the recording medium as well and are subjected to interanthentication with the device side every time the means are mounted at the recording and reproducing device. Whether the device and medium have the adequate rights with each other or not is inspected. As to the data used by adequate right processing, use history information is previously stored and finally approval is effected by third party organizations.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－332023
（P2001－332023A）
(43)公開日　平成13年11月30日(2001.11.30)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10		Ｈ　５Ｄ０４４
19/02	５０１	19/02	５０１Ｊ	５Ｄ０６６

審査請求　未請求　請求項の数25　ＯＬ　（全 32 頁）

(21)出願番号　特願2000－152788(P2000－152788)

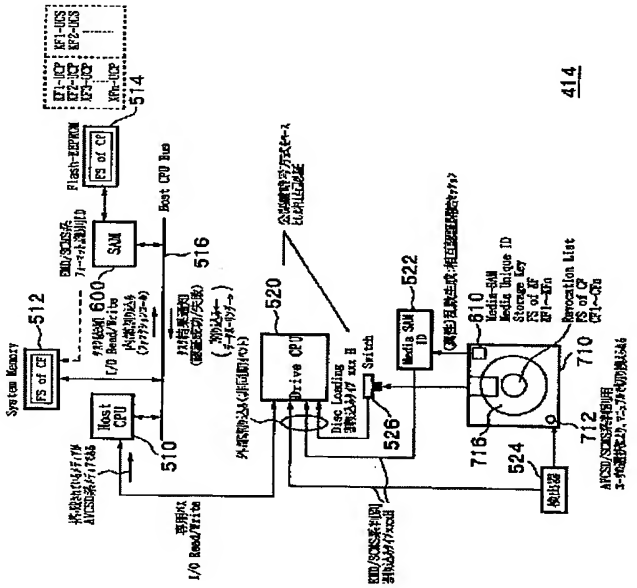
(22)出願日　平成12年５月19日(2000.5.19)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(72)発明者　野中　聡
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　江崎　正
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100094053
弁理士　佐藤　隆久

Ｆターム(参考)　5D044 CC04 DE49 DE50 EF05 FG18
GK17 HL08
5D066 DA03 DA12 DA16

(54)【発明の名称】　データ記録装置、データ再生装置、データ処理装置およびデータ記録媒体

(57)【要約】
【課題】適切に権利処理を行いながらデータを記録再生する記録装置、再生装置、データを配信するデータ処理装置および記録媒体を提供する。
【解決手段】データは暗号化して配信し、各機器に搭載されたセキュアな処理手段で権利処理を行い、適切な権利の場合にのみ記録、再生を行なう。記録媒体にも、鍵データや認証手段などを有するセキュアな処理手段を搭載し、記録再生装置に搭載されるごとに、装置側と相互認証を行い、相互に適切な権利を有する装置、媒体であるか検査する。適切に権利処理して使用されたデータについては、使用履歴情報を蓄積しておき、最終的に第三者機関で決済を行なう。



1

【特許請求の範囲】

【請求項１】装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、
前記記録媒体が適切な場合に、入力される暗号化された配信対象のデータを、入力される当該データの使用条件の範囲内で前記記録媒体に記録する記録手段と、
前記記録に係わる係わる使用履歴情報を記憶する手段と、
前記使用履歴情報を所定の送信先に送信する送信手段とを有するデータ記録装置。

【請求項２】前記記録媒体検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査する請求項１に記載のデータ記録装置。

【請求項３】前記記録媒体検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査する請求項１に記載のデータ記録装置。

【請求項４】前記装着された前記記録媒体の所定の物理形状を検出する形状検出手段を有し、
前記記録媒体検査手段は、前記検出された前記装着された記録媒体の所定の形状に基づいて、当該データ記録媒体が適切な転送先か否かを検査する請求項１に記載のデータ記録装置。

【請求項５】前記記録媒体検査手段は、外部より観察不可能な状態で前記各処理を行なう請求項３に記載のデータ記録装置。

【請求項６】前記記憶手段は、前記記録媒体が適切な場合に、入力される暗号化された配信対象のデータを利用するための鍵データをさらに記憶する請求項１に記載のデータ記録装置。

【請求項７】前記記録媒体に記録された鍵データを読み出す鍵データ読み出し手段と、
前記記録媒体に記録された暗号化された配信対象のデータを読み出すデータ読み出し手段と、
前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、
前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段とをさらに有し、
前記使用履歴情報記憶手段は、前記再生の履歴情報をさらに記憶する請求項６に記載のデータ記録装置。

【請求項８】前記鍵データ読み出し手段は、前記読み出した鍵データを、外部より観察不可能なセキュアな記憶領域に記憶する請求項７に記載のデータ記録装置。

【請求項９】前記使用条件の情報は、当該配信対象の使用許可条件、対価、権利処理情報、課金条件の少なくともいずれかを含み、
前記使用手段は、前記制御情報に基づいて前記データを使用し、当該使用に係わる使用履歴情報を通知する請求項１に記載のデータ記録装置。

2

【請求項１０】前記配信対象のデータは、音楽データ、画像データ、映像（動画像）データ、オーディオデータおよび映像データを含むビデオデータ、コンピュータプログラムデータ、コンピュータデータを含むコンテンツデータのいずれかである請求項１に記載のデータ記録装置。

【請求項１１】装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、
前記記録媒体が適切な場合に、前記記録媒体より鍵データを読み出す鍵データ読み出し手段と、
前記記録媒体が適切な場合に、前記記録媒体より暗号化された配信対象のデータを読み出すデータ読み出し手段と、
前記記録媒体が適切な場合に、前記記録媒体より前記配信対象のデータの使用条件の情報を読み出す使用条件読み出し手段と、前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、
前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段と前記再生の履歴情報を記憶する使用履歴情報記憶手段と、
前記記憶した使用履歴情報を所定の送信先に送信する送信手段とを有するデータ再生装置。

【請求項１２】配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、
前記受信した配信データを蓄積する蓄積手段と、
前記受信した鍵データに基づいて、前記暗号化された配信データを復号化する復号化手段と、
前記復号化された配信データに含まれる使用条件の情報に従って、前記配信対象のデータを使用可能な状態とする第１の使用手段と、
任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、
前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記使用可能な状態とされた配信データを配信するデータ転送手段とを有するデータ処理装置。

【請求項１３】前記第１の使用手段における前記使用に係わる履歴情報を記憶する使用履歴情報記憶手段と、
前記記憶した使用履歴情報を所定の送信先に送信する送信手段とをさらに有する請求項１２に記載のデータ処理装置。

【請求項１４】前記使用可能な状態とされた配信対象のデータを使用する第２の使用手段をさらに有する請求項１２に記載のデータ処理装置。

【請求項１５】前記第１の使用手段および前記第２の使用手段における前記使用に係わる履歴情報を記憶する使用履歴情報記憶手段と、
前記記憶した使用履歴情報を所定の送信先に送信する送

信手段とをさらに有する請求項１３に記載のデータ処理装置。

【請求項１６】前記復号手段、前記第１の使用手段、前記転送先検査手段、前記第２の使用手段および前記使用履歴情報記憶手段は、外部より観察不可能な状態で前記各処理を行なう請求項１５に記載のデータ処理装置。

【請求項１７】前記データ転送先は、データ記録装置であって、

前記転送先検査手段は、前記データ記録装置と相互認証を行なうことにより、当該データ記録装置が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録装置が適切であった場合に、前記使用可能な状態とされた前記配信データを配信する請求項１３に記載のデータ処理装置。

【請求項１８】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記使用可能な状態とされた前記配信データを当該データ記録媒体に記録する請求項１３に記載のデータ処理装置。

【請求項１９】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記使用可能な状態とされた前記配信データを当該データ記録媒体に記録する請求項１３に記載のデータ処理装置。

【請求項２０】配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、

前記受信した配信データを蓄積する蓄積手段と、

任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、

前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記配信データを配信するデータ転送手段とを有するデータ処理装置。

【請求項２１】前記転送先検査手段は、外部より観察不可能な状態で、前記データ転送先が前記配信データの転送先として適切か否かを検査する請求項２０に記載のデータ処理装置。

【請求項２２】前記データ転送先は、データ記録装置であって、

前記転送先検査手段は、前記データ記録装置と相互認証

を行なうことにより、当該データ記録装置が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録装置が適切であった場合に、前記配信データを配信する請求項２１に記載のデータ処理装置。

【請求項２３】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記配信データを当該データ記録媒体に記録する請求項２１に記載のデータ処理装置。

【請求項２４】前記データ転送先は、データ記録媒体であって、

前記転送先検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査し、

前記データ転送手段は、前記データ記録媒体が適切であった場合に、前記配信データを当該データ記録媒体に記録する請求項２１に記載のデータ処理装置。

【請求項２５】任意のデータを記録するデータ記録領域と、

装着されたデータ処理装置と通信を行い相互認証を行なう相互認証手段と、

前記認証の結果適切と判定されたデータ処理装置にのみアクセスされるデータを記録するデータ記録手段とを有するデータ記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、たとえば、音声や映像など種々の種類の信号、種々の仕様の機器、種々の信号諸元あるいは種々の権利関係などが混在し、ネットワークやパッケージメディアなど種々の媒体を介して配信されるデータ配信システムにおいて用いて好適な、データ記録装置、データ再生装置、データ処理装置およびデータ記録媒体に関する。

【０００２】

【従来の技術】デジタル信号処理技術の急速な進展により、音楽データなどはデジタル信号として扱われ、ＭＤやＤＶＤなどに記録され、利用されるようになっている。さらに、これまでデータ量が膨大になるため敬遠されていた画像データも、デジタルデータとして扱われ、ランダムアクセス可能なディスク型の記録媒体や半導体メモリを用いた記録媒体に記録されるようになりつつある。一方で、通信技術および情報処理技術の進展により、インターネットを初めとする通信ネットワークの普及も著しい。そして、近年の通信速度や端末装置の性能の飛躍的な向上により、そのような通信ネットワークに

5

おいては、個人間のメール転送やニュースの配信というような利用形態にとどまらず、前述したようなデジタル形式の音楽データ、ビデオデータあるいはコンピュータプログラムデータなどを配信できる環境となっている。

【０００３】

【発明が解決しようとする課題】ところで、そのようなデジタル形式の音楽データやビデオデータは、コピーを行なっても品質が劣化しないことから、著作権などを無視した不正なコピーが次々と行なわれる危険性がある。したがって、前述したようなネットワークを介したデータ配信においても、適切にデータの使用がコントロールされ、データの使用に基づく利益が適切に権利者に還元されるような仕組みを作ることが重要である。

【０００４】したがって、本発明の目的は、所望のデータを、適切に権利処理を行いながら記録することのできるデータ記録装置を提供することにある。また本発明の目的は、記録された所望のデータを、適切に権利処理を行いながら再生することのできるデータ再生装置を提供することにある。また、本発明の他の目的は、所望のデータを、任意の信号諸元で任意の媒体、通信路、機器を介して任意の配信先に所定の権利処理を行いながら配信するためのデータ処理装置を提供することにある。さらに本発明の他の目的は、所望のデータを、適切に権利処理を行いながら記録および再生することのできるデータ記録媒体を提供することにある。

【０００５】

【課題を解決するための手段】したがって、本発明のデータ記録装置は、装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、前記記録媒体が適切な場合に、入力される暗号化された配信対象のデータを、入力される当該データの使用条件の範囲内で前記記録媒体に記録する記録手段と、前記記録に係わる係わる使用履歴情報を記憶する手段と、前記使用履歴情報を所定の送信先に送信する送信手段とを有する。

【０００６】好適には、前記記録媒体検査手段は、前記データ記録媒体と相互認証を行なうことにより、当該データ記録媒体が適切な転送先か否かを検査する。また好適には、前記記録媒体検査手段は、前記データ記録媒体の所定のセキュアな記録領域より所定の識別情報を読み出し、該読み出した識別情報に基づいて当該データ記録媒体が適切な転送先か否かを検査する。また好適には、前記装着された前記記録媒体の所定の物理形状を検出する形状検出手段を有し、前記記録媒体検査手段は、前記検出された前記装着された記録媒体の所定の形状に基づいて、当該データ記録媒体が適切な転送先か否かを検査する。さらに好適には、前記記録媒体検査手段は、外部より観察不可能な状態で前記各処理を行なう。

【０００７】また好適には、前記記憶手段は、前記記録媒体が適切な場合に、入力される暗号化された配信対象のデータを利用するための鍵データをさらに記憶する。また好適には、前記記録媒体に記録された鍵データを読み出す鍵データ読み出し手段と、前記記録媒体に記録された暗号化された配信対象のデータを読み出すデータ読み出し手段と、前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段とをさらに有し、前記使用履歴情報記憶手段は、前記再生の履歴情報をさに記憶する。好適には、前記鍵データ読み出し手段は、前記読み出した鍵データを、外部より観察不可能なセキュアな記憶領域に記憶する。

6

【０００８】特定的には、前記使用条件の情報は、当該配信対象の使用許可条件、対価、権利処理情報、課金条件の少なくともいずれかを含み、前記使用手段は、前記制御情報に基づいて前記データを使用し、当該使用に係わる使用履歴情報を通知する。また特定的には、前記配信対象のデータは、音楽データ、画像データ、映像（動画像）データ、オーディオデータおよび映像データを含むビデオデータ、コンピュータプログラムデータ、コンピュータデータを含むコンテンツデータのいずれかである。

【０００９】また本発明のデータ再生装置は、装着された記録媒体が適切な処理対象の記録媒体か否かを検査する記録媒体検査手段と、前記記録媒体が適切な場合に、前記記録媒体より鍵データを読み出す鍵データ読み出し手段と、前記記録媒体が適切な場合に、前記記録媒体より暗号化された配信対象のデータを読み出すデータ読み出し手段と、前記記録媒体が適切な場合に、前記記録媒体より前記配信対象のデータの使用条件の情報を読み出す使用条件読み出し手段と、前記鍵データに基づいて前記暗号化された配信対象のデータを復号化する復号化手段と、前記使用条件の情報に従って、前記復号化された配信対象のデータを再生する再生手段と前記再生の履歴情報を記憶する使用履歴情報記憶手段と、前記記憶した使用履歴情報を所定の送信先に送信する送信手段とを有する。

【００１０】また、本発明のデータ処理装置は、配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、前記受信した配信データを蓄積する蓄積手段と、前記受信した鍵データに基づいて、前記暗号化された配信データを復号化する復号化手段と、前記復号化された配信データに含まれる使用条件の情報に従って、前記配信対象のデータを使用可能な状態とする第１の使用手段と、任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記使用可能な状態とされた配信デ

ータを配信するデータ転送手段とを有する。

【００１１】また、本発明の他のデータ処理装置は、配信される、暗号化された配信対象のデータと当該データの使用条件の情報を含む暗号化された配信データ、および、前記配信データを利用するための鍵データを、各々受信する受信手段と、前記受信した配信データを蓄積する蓄積手段と、任意のデータ転送先が、前記配信データの転送先として適切か否かを検査する転送先検査手段と、前記検査の結果、前記データ転送先が適切であった場合に、少なくとも前記配信データを配信するデータ転送手段とを有する。

【００１２】また、本発明のデータ記録媒体は、任意のデータを記録するデータ記録領域と、装着されたデータ処理装置と通信を行い相互認証を行なう相互認証手段と、前記認証の結果適切と判定されたデータ処理装置にのみアクセスされるデータを記録するデータ記録手段とを有する。

【００１３】

【発明の実施の形態】本発明の一実施の形態について、図１～図４６を参照して説明する。本実施の形態においては、音楽データを処理する装置であって、ネットワークを介して配信される音楽データを受信し利用可能な状態するデータ処理装置、そのような音楽データの利用装置としてのデータ記録装置、データ再生装置およびデータ記録再生装置などを例示して、本発明を説明する。なおここでは、本発明に係わる、音楽データを適正に利用するための権利処理や構成を中心に説明する。したがって、通常の音楽データの記録あるいは再生装置が有する通常の構成については、その詳細な説明を省略する。

【００１４】ＥＭＤシステム

まず、本発明に係わる各装置が使用される環境であり、音楽データをネットワークあるいはパッケージメディアを介して、適正な権利処理を行いながら配信する電子音楽配信システム（ＥＭＤ(Electronic Music Distribution) システム）について説明する。

【００１５】ＥＭＤシステムの構成

まず、そのＥＭＤシステム１の全体構成について図１を参照して説明する。図１は、そのＥＭＤシステム１の構成を示すブロック図である。ＥＭＤシステム１は、ＥＭＤサービスセンタ１００、コンテンツプロバイダ２００、サービスプロバイダ２５０、デリバリチャネル３００、ユーザホームネットワーク４００を有する。なお、図１に示すＥＭＤシステム１は、ＥＭＤサービスセンタ１００、コンテンツプロバイダ２００およびサービスプロバイダ２５０を各々１つ、ユーザホームネットワーク４００を２つ有する構成であるが、これは説明に好適な構成であって、後に各々説明するように、各構成部の数は各々任意でよい。

【００１６】ＥＭＤサービスセンタ１００

ＥＭＤサービスセンタ１００は、音楽コンテンツデータが、適切に権利処理され、適切に課金処理され、そして適切に利益分配されながら適切に配信されるように、ＥＭＤシステム１全体を管理する。

【００１７】具体的には、まずＥＭＤサービスセンタ１００は、コンテンツプロバイダ２００、サービスプロバイダ２５０、ユーザホームネットワーク４００のユーザおよび各機器を初めとして、メディアや図示せぬポータルなど、音楽コンテンツデータの配信に関わる全てのエンティティについて、それらの登録を受け付け、ＩＤを割り当て、種々の属性や後の利益分配に用いる決裁口座の口座番号などの情報をデータベースとして蓄積し管理する。特に、本発明に係わる、ＳＡＭを実質的に搭載しセキュアな状態で権利処理が可能となっているＥＭＤシステム対応機器（以後、ＥＭＤハードウエアと言う場合もある。）については、基本的にその全ての機器の情報がＥＭＤサービスセンタ１００に登録され管理される。

【００１８】またＥＭＤサービスセンタ１００は、それら各エンティティが、たとえばデータを伝送する際に用いる鍵データや証明書データなどを管理し、それらの正当性を証明する処理などを行なう。またＥＭＤサービスセンタ１００は、コンテンツプロバイダ２００にコンテンツを暗号化して配信するためのディストリビューション鍵を配付するとともに、ユーザホームネットワーク４００にその暗号を解読するためのディストリビューション鍵を適正な権利処理を条件に使用できる状態で配付することにより、コンテンツの配信をコントロールする。

【００１９】またＥＭＤサービスセンタ１００は、コンテンツプロバイダ２００より、配信対象の音楽コンテンツデータに関わる情報、その各音楽コンテンツデータごとの配信に関わった各エンティティに対する利益分配の割合を示す利益分配データ、および、その各音楽コンテンツデータの配信の際の信号諸元に対応した価格を規定した価格換算データの登録を受け付け、これらを管理する。そしてＥＭＤサービスセンタ１００は、ユーザホームネットワーク４００からコンテンツの利用に応じて逐次送信されるコンテンツ使用情報（Usage-Log ）を受信し、前述した利益分配データおよび価格換算データを参照して、そのコンテンツの制作から流通に係わった各エンティティへの利益の配分処理を行なう。

【００２０】なお、このＥＭＤサービスセンタ１００は、各ＥＭＤシステム１ごとに１つ存在するのが好適である。

【００２１】コンテンツプロバイダ２００

コンテンツプロバイダ２００は、基本的に音楽コンテンツデータの著作権者であり、配信対象の配信コンテンツデータに対して、図２に示すようなコンテンツプロバイダセキュアコンテナを生成し、配信業者であるサービスプロバイダ２５０に供給する。具体的には、コンテンツプロバイダ２００は、コンテンツデータに、自己のコンテンツであることを証明するための著作権情報をウォー

ターマーク情報（電子透かし情報）として重畳し、さらに、アナログインターフェイス経由でのコピーを禁止するためのコピー禁止ビットが埋め込まれているウォーターマーク情報を重畳し、そのコンテンツデータを圧縮して、自らが生成したコンテンツ鍵で暗号化する。

【００２２】また、そのコンテンツに関する取扱方針を定めた使用許諾条件（ＵＣＰ：Usage Control Policy）を作成し、ＥＭＤサービスセンタ１００から配信されたディストリビューション鍵でコンテンツ鍵およびＵＣＰを暗号化する。そして、コンテンツ鍵で暗号化されたコンテンツと、ディストリビューション鍵で暗号化されたコンテンツ鍵とＵＣＰに対して、各々ハッシュ値をとり、コンテンツプロバイダ２００の秘密鍵を用いて署名を生成する。この署名を、先の各データに添付してコンテンツプロバイダセキュアコンテナを生成し、サービスプロバイダ２５０に供給する。

【００２３】また、コンテンツプロバイダ２００は、コンテンツプロバイダセキュアコンテナを生成して音楽コンテンツデータを配信対象としたら、その音楽コンテンツデータに関わる情報、その各音楽コンテンツデータごとの配信に関わった各エンティティに対する利益分配の割合を示す利益分配データ、および、その各音楽コンテンツデータの配信の際の信号諸元に対応した価格を規定した価格換算データをＥＭＤサービスセンタ１００に送信し、登録する。登録した情報およびデータは、その音楽コンテンツデータが利用された場合の課金処理および利益配分の際に使用される。

【００２４】なお、コンテンツプロバイダ２００は、たとえば従来のレコード会社に相当するような、著作権を保持してコンテンツを管理している団体ごとに存在するものであり、１つのＥＭＤシステム１に対して多数存在するものである。

【００２５】サービスプロバイダ２５０

サービスプロバイダ２５０は、コンテンツプロバイダ２００から供給されたコンテンツプロバイダセキュアコンテナに対して、図３に示すようなサービスプロバイダセキュアコンテナを生成し、任意のデリバリチャネル３００を介してユーザホームネットワーク４００-1に配信する。具体的には、サービスプロバイダ２５０は、ＥＭＤサービスセンタ１００より供給されるコンテンツプロバイダ２００の公開鍵によりコンテンツプロバイダセキュアコンテナの署名検証を行う。

【００２６】次に、自分が行なう配信サービスの利益分を上乗せした新たな価格情報（ＰＴ：Price Tag ）を付加し、これらのデータ各々のハッシュ値をとり、サービスプロバイダ２５０の秘密鍵を用いて署名を生成する。この署名を、先の各データに添付してサービスプロバイダセキュアコンテナを生成し、デリバリチャネル３００を介してユーザホームネットワーク４００に配信する。なお、このサービスプロバイダ２５０も、１つのＥＭＤシステム１に対して多数存在するものである。

【００２７】デリバリチャネル３００

デリバリチャネル３００は、任意の配信チャネルを示す。具体的には、インターネットなどの通信ネットワーク、ケーブルテレビジョンシステム、衛星放送システム、ＡＴＭ通信網、移動帯通信網、パッケージメディアによる配信など、任意の配信手段を含む。

【００２８】ユーザホームネットワーク４００

ユーザホームネットワーク４００-1，４００-2は、サービスプロバイダ２５０から配信されたサービスプロバイダセキュアコンテナを受信し、必要に応じてその中に含まれえるコンテンツデータを実際に使用する。ユーザホームネットワーク４００の一般的な構成を図４に示す。ユーザホームネットワーク４００は、各家庭ごとの音楽データの記録あるいは再生を行なう装置群であると考えるのが好適であるが、厳密には、家庭内、家庭外を問わず、任意の種々の装置により構成されるものである。より具体的には、ユーザホームネットワーク４００に接続される機器としては、データ記録装置、再生装置、記録再生装置などであり、これらの各装置が、本発明に係わる装置である。

【００２９】なお、以下の説明においては、説明を容易にするために、便宜上これらの機器を、通信機能を有しているネットワーク機器４１０と、それ自体は通信機能をもっておらず記録媒体を介して音楽データの記録および再生を行なう記録再生装置４１２とに分類する。すなわち、図４に示す第１のユーザホームネットワーク４００-1は、２台のネットワーク機器４１０-1，４１０-2と、２台の記録再生装置４１２-1，４１２-2を有し、第２のユーザホームネットワーク４００-2は、３台のネットワーク機器４１０-3～４１０-5と、４台の記録再生装置４１２-3～４１２-6を有する。そして、ネットワーク機器４１０の間は通信回線によるコンテンツデータの転送が可能であるが、記録再生装置４１２間では、記録メディア７００を介してコンテンツデータが移動されることになる。

【００３０】これらの各機器には、いずれも後述するＳＡＭ（Secure Application Module）チップと言われる、暗号化されたコンテンツデータの復号化および課金処理およびコピーコントロールを含む適正な権利処理を行なうためのチップが搭載されており、このチップにより適正に権利処理を行いながら音楽データの記録および再生を行なわれるようになっている。前述した、ＥＭＤサービスセンタ１００からユーザホームネットワーク４００に配信されるディストリビューション鍵は、各機器のこのＳＡＭチップに格納されている。また、各ユーザホームネットワーク４００には、ＥＭＤサービスセンタ１００と通信可能なにネットワーク機器４１０が少なくとも１台は設けられており、このネットワーク機器４１０を介して、そのユーザホームネットワーク４００にお

けるコンテンツの使用履歴情報が、ＥＭＤサービスセンタ１００に通報されるようになっている。

【００３１】さて、このようなユーザホームネットワーク４００において、いずれかのネットワーク機器４１０がデリバリチャネル３００よりサービスプロバイダセキュアコンテナを受信すると、ネットワーク機器上のダウンロードメモリに一旦格納され、ＥＭＤサービスセンタ１００より供給されるサービスプロバイダ２５０の公開鍵により署名検証が行なわれる。そして、各機器からの再生要求などに応じて、購入形態が決定されると、後述する使用状態情報（ＵＣＳ：Usage Control Status）が生成され、ＳＡＭでディストリビューション鍵が外され、課金情報となる使用履歴情報（Usage Log ）がＳＡＭに蓄積されて、実質的にそのコンテンツが購入される。なお、蓄積された使用理例情報は、適宜ＥＭＤシステム１０に送信され、課金および決済処理に用いられる。購入されたコンテンツデータは、たとえば記録媒体などに依存したストレージ鍵により新たに鍵がかけられ、サービスプロバイダセキュアコンテナと同様に署名データが付されて、図５に示すようなユーザホームネットワークセキュアコンテナの形態で、以後、ユーザホームネットワーク４００の中で流通される。

【００３２】セキュアコンテナ

このように、ＥＭＤシステム１においては、コンテンツデータは、図２に示したコンテンツプロバイダセキュアコンテナ、図３に示したサービスプロバイダセキュアコンテナ、そして、図５に示したユーザホームネットワークセキュアコンテナという、セキュアコンテナという形態で伝送される。各セキュアコンテナの構造については前述した通りだが、ここでは、各セキュアコンテナに含まれるＵＣＰおよびＵＣＳについて説明する。

【００３３】ＵＣＰ

ＵＣＰは、コンテンツプロバイダ２００によって与えられる、そのコンテンツデータの配信方針、取扱方針が記されたデータである。ＵＣＰの具体的な内容を図６に示す。図示のごとく、ＵＣＰには、そのコンテンツデータを特定するＩＤ、コンテンツプロバイダ２００およびＥＭＤサービスセンタ１００の各署名データ、そのコンテンツデータの配信に係わる種々の情報、コンテンツの内容や属性に関する種々の情報、後述する利用空間調査に対する取扱制御情報、種々の課金時の条件に基づく取扱制御情報、および、そのコンテンツデータの使用形態および課金データのなどの情報が記されている。そして特に、本発明に係わる情報としては、コンテンツデータの信号諸元や圧縮方式などの情報、利用空間調査結果に対する取扱制御情報、および、各購入形態に対する取扱方針や価格情報を記録した使用制御情報が、このＵＣＰに記録されている。

【００３４】ＵＣＳ

ＵＣＳは、コンテンツデータを購入する際に生成去れる使用状態を示すためのデータである。ＵＣＳの具体的な内容を図７に示す。図示のごとく、ＵＣＳには、コンテンツプロバイダ２００、ＥＭＤサービスセンタ１００およびサービスプロバイダ２５０の各ＩＤおよび署名、および、その購入に関する購入者ＩＤ、決裁手段、販売価格、種々のディスカウントに係わる情報などが記されている。そして特に、本発明に係わる情報としては、後述する利用空間情報の調査結果が、このＵＣＳに記録されている。

【００３５】ホームネットワーク機器

次に、本発明に係わる、このようなＥＭＤシステム１のユーザホームネットワーク４００において用いられる、代表的な機器についてその構成を説明する。図８は、ＳＡＭを収容する記録メディア７１０に対してデータの記録および再生を行なう記録再生機器４１４の主要部の構成を示す図である。記録再生機器４１４は、ホストＣＰＵ５１０、システムメモリ５１２、ＳＡＭ６００、フラッシュＥＥＰＲＯＭ５１４、ドライブＣＰＵ５２０、メディアＳＡＭＩ／Ｆ５２２、ＥＭＤ系メディア検出器５２４およびメディア検出スイッチ５２６を有する。

【００３６】ホストＣＰＵ５１０は記録再生機器４１４全体を制御するＣＰＵである。システムメモリ５１２は、ホストＣＰＵ５１０における種々の処理に用いられるメモリであり、記録メディア７１０が装着された際には、コンテンツファイルのファイルシステムが記録される。ＳＡＭ６００はコンテンツデータの権利処理および復号処理などの処理を行なうチップである。ＳＡＭ６００は、メディア検出スイッチ５１６によりホストＣＰＵ５１０と接続されており、ホストＣＰＵ５１０からはＩ／Ｏとして制御される。すなわち、Ｉ／Ｏライトにより ＳＡＭ６００にタスク依頼がなされ、またＩ／Ｏリードによりタスクの結果がセンスされる。フラッシュＥＥＰＲＯＭ５１４は、ＳＡＭ６００の外付けメモリであり、記録メディア７１０が装着された場合には、鍵ファイルのファイルシステムが記録される。

【００３７】ドライブＣＰＵ５２０は、記録メディアに対するリード／ライト全般を制御する制御部である。ドライブＣＰＵ５２０は、ホストＣＰＵ５１０と専用バスにより接続されている。メディアＳＡＭＩ／Ｆ５２２は、記録メディア７１０のメディアＳＡＭ６１０と通信を行なうためのインターフェイスである。ＥＭＤ系メディア検出器５２４は、記録メディア７１０のマニュアルスイッチの位置を検出し、記録メディア７１０がＥＭＤ系メディアとして用いられているのかＳＣＭＳ系メディアとして用いられているのかを検出する。メディア検出スイッチ５２６は、記録再生機器４１４に記録メディア７１０が装着されたことを検出するスイッチである。

【００３８】このような記録再生機器４１４に装着される記録メディア７１０は、図示のごとく、メディアＳＡＭ６１０を有するＥＭＤ系メディアである記録メディア

７１０が装着される。記録メディア７１０において、メディアＳＡＭ６１０においては、装着される記録再生機器４１４の正当性のチェックや、記録されているコンテンツデータに係わる権利処理などが行なわれる。また、メディアＳＡＭ６１０には、メディアのユニークＩＤ、ストレージ鍵、鍵ファイルのファイルシステムおよび鍵ファイルなどが記憶される。また、記録メディア７１０のＲＡＭ領域７１６には、適切でない機器のリストであるリボケーションリスト、コンテンツファイルのファイルシステムおよびコンテンツファイルが記録される。また、この記録メディア７１０は、ＳＣＭＳ系メディアとして使用するのかＥＭＤ系メディアとして使用するのかを指定するためのマニュアルスイッチ７１２が設けられている。

【００３９】また、図９は、ＳＡＭは実装していないもののセキュアなＲＡＭ領域を有する記録メディア７２０に対して、データの記録および再生を行なう記録再生機器４１６の主要部の構成を示す図である。記録再生機器４１６は、ホストＣＰＵ５１０、システムメモリ５１２、ＳＡＭ６００、フラッシュＥＥＰＲＯＭ５１４、ドライブＣＰＵ５２０およびドライブＬＳＩ５２８を有する。ホストＣＰＵ５１０、システムメモリ５１２、ＳＡＭ６００、フラッシュＥＥＰＲＯＭ５１４およびドライブＣＰＵ５２０の構成は、前述した記録再生機器４１４の構成と同じである。ドライブＬＳＩ５２８は、記録メディア７２０のＲＯＭ領域７２２およびセキュアＲＡＭ領域７２４にアクセスをするためのドライブ回路である。

【００４０】そして、このようなドライブＬＳＩ５２８を介して、記録メディア７２０のＲＯＭおよびセキュアＲＡＭ領域にメディアのユニークＩＤ、ストレージ鍵、鍵ファイルのファイルシステムおよび鍵ファイルなどを記憶することにより、メディアＳＡＭ６１０が実装されていなくとも、記録メディア７２０をＥＭＤ系メディアとして扱うことができる。また、記録メディア７２０では乱数生成の必要なストレージ鍵の生成は、行なえないため、ドライブＬＳＩ５２８は、ストレージ鍵の生成処理も行なう。

【００４１】なお、このようなホームネットワーク機器には、必要に応じて、たとえば図１０あるいは図１１に示すような構成のＳＡＭ６００、図１２に示すようなＡＶコーデックＳＡＭ６２０、および、図１３あるいは図１４に示すような構成のドライブＳＡＭ６３０が搭載される。また、記録メディア７１０には、図１５あるいは図１６に示すようなメディアＳＡＭ６１０が搭載される。

【００４２】利用空間調査

概要

さて、前述したようなユーザホームネットワーク４００の各機器においては、全ての機器にＳＡＭが搭載されて

おり、これにより適正に権利処理が行なわれ、コンテンツファイルがハンドリングされるものとした。しかしながら、実際の家庭には、アナログ機器や、ＳＣＭＳビットによりコピーコントロールを行なうＳＣＭＳ機器などが多数存在している。また記録メディアにおいても、単なるＲＡＭ領域しか形成されていな記録メディアが多数普及している。すなわち、実際には、これらの機器や記録メディアをも含めた形態で、ユーザホームネットワーク４００が構成されている場合が多い。また一方で、ＥＭＤシステム１だけを見ても、これは使用できる記録メディアや使用できるコンテンツデータの信号諸元、圧縮・符号化方式などを何ら限定されるものではない。したがって、種々の信号諸元で種々の方式により圧縮符号化されたコンテンツデータが使用されている。

【００４３】そのような環境の下で、たとえば図１７に示すようにあるパッケージメディアのコンテンツデータを、他の記録メディアにコピーしようとした場合には、再生側の記録メディア、再生側の機器、記録側の機器そして記録側の記録メディアと、各機器、メディアの仕様を全て把握し、さらに記録されているコンテンツデータの信号諸元や圧縮符号化方式などを把握するした上でなければ、最適な条件でコピーを行なうことはできない。さらに、そのような条件を全て把握した状態でなければ、適切な権利処理を行ない適切に利益分配を行なうこともできない。

【００４４】そこで、ＥＭＤシステム１においては、このようなコピーを行なう前に、利用空間調査と称して、記録側および再生側の機器、記録メディア、信号諸元、圧縮符号化方式、さらには、権利処理方式などまでをも調査し、把握するようにしている。以下、この利用空間調査の方法、および、利用空間調査を行なった上でのコンテンツデータのコピーなどの処理について説明する。

【００４５】利用空間調査

本実施の形態のＥＭＤシステム１において、利用空間調査とは、各機器およびＳＡＭにおいて、次の４つの観点から行なう。

【００４６】１．ＥＭＤ系かＳＣＭＳ系かの調査

まず第１は、処理対象のコンテンツ、ハードウェア（機器）および記録メディアが、各々、ＥＭＤシステム１に適合したＥＭＤ系のものか、ＥＭＤシステム１に適合していない従来のＳＣＭＳ系のものかを調査し、これにより記録／再生をコントロールし、権利処理、コピーコントロールおよび利益分配が適切に遂行されるようにする。

【００４７】ここで、コンテンツ、ハードウエアおよび記録メディアのＥＭＤ系およびＳＣＭＳ系は、次のように定義する。ＥＭＤ系コンテンツとは、暗号化され、鍵ファイルとともに流通されるコンテンツである。ＳＣＭＳ系コンテンツとは、非暗号化された状態で、ＳＣＭＳビットによりコピーコントロールされる状態で流通され

15　　16

るコンテンツである。ＥＭＤ系ハードウエアとは、ＳＡＭが搭載されており、ＳＡＭによる権利処理が行なえる機器である。

【００４８】ＳＣＭＳ系ハードウエアとは、ＳＣＭＳビットによるコピーコントロールに対応している機器である。ＥＭＤ系メディアとは、何らかの形で記録メディア上で認証機能を有するメディアであり、２つの形態がある。１つは、ＳＡＭ（メディアＳＡＭ）が搭載され、これにより認証機能を実現するメディアであり、もう１つは、メディア上にセキュアＲＡＭ領域を持ち、このセキュアＲＡＭ領域を用いて外部からの処理により認証機能を実現するメディアである。ＳＣＭＳ系メディアとは、ＳＣＭＳビットのみを有するメディアである。

【００４９】そして、これまでに説明したような権利処理およびコピーコントロールを適切に行なうためには、これら各コンテンツ、ハードウエアおよび記録メディア間の記録および再生は、次表１のように規定するとが望ましい。

【００５０】

【表１】

	ＳＣＭＳ系メディア		ＥＭＤ系メディア	
	ＥＭＤ系コンテンツ	ＳＣＭＳ系コンテンツ	ＥＭＤ系コンテンツ	ＳＣＭＳ系コンテンツ
ＳＣＭＳ系ハードウエア	×	○	×	○
ＥＭＤ系ハードウエア	×	○	○	○

【００５１】表１の各項目について順に説明する。まず、テーブルの左上の条件、すなわち、ＳＣＭＳ系メディアとＳＣＭＳ系ハードウエアの組み合わせに対して、暗号化コンテンツおよび鍵ファイルからなるＥＭＤ系コンテンツを記録あるいは再生する場合、この場合は、ＥＭＤ系コンテンツの暗号化コンテンツをＳＣＭＳ系ハードウエアでは処理できないので、仮にＳＣＭＳ系メディアにＥＭＤ系コンテンツが記録されていたとしても再生できないし、新たにＥＭＤ系コンテンツを記録することもできない。

【００５２】次に、左下の条件、すなわち、ＳＣＭＳ系メディアとＥＭＤ系ハードウエアの組み合わせに対して、ＥＭＤ系コンテンツを記録あるいは再生する場合、この場合は、技術的には単に記録し再生するという処理は可能である。しかしながら、ＳＣＭＳ系メディアという、何ら権利処理に係わる構成、セキュアな処理に対応した構成を保持していない媒体に対してそのような処理を行なうことは、ＥＭＤシステム１の権利処理を無効にし、虚偽の処理や不正な流通を発生させる原因となるものである。したがって、ＳＣＭＳ系メディアへのＥＭＤ系コンテンツの記録、また、仮に記録されていたとしても、ＳＣＭＳ系メディアからのＥＭＤ系コンテンツの再生は、行なえないようにするのが適切である。

【００５３】次に、ＳＣＭＳ系メディアとＳＣＭＳ系ハードウエアの組み合わせに対して、ＳＣＭＳ系コンテンツを記録あるいは再生する場合、この場合は、従来のＳＣＭＳビットによるコピーコントロールシステムと同じであり、再生および記録ともそのＳＣＭＳビットに従って可能である。また、ＳＣＭＳ系メディアをＥＭＤ系ハードウエアに装着した場合にＳＣＭＳ系コンテンツを記録あるいは再生する場合、この場合は、ＥＭＤ系ハードウエアの仕様として、記録あるいは再生を、行なえるようにしてもよいし、行なえないようにしてもよいが、記録メディアの上位互換性という観点において、再生および記録とも可能にしておくのが好適である。

【００５４】次に、ＥＭＤ系メディアとＳＣＭＳ系ハードウエアの組み合わせに対してＥＭＤ系コンテンツを記録あるいは再生する場合、この場合も、前述したＳＣＭＳ系メディアとＳＣＭＳ系ハードウエアに対するＥＭＤ系コンテンツの記録／再生の場合と同様に、ＥＭＤ系コンテンツの暗号化コンテンツをＳＣＭＳ系ハードウエアでは処理できないので、記録および再生とも不可能である。次に、ＥＭＤ系メディアとＥＭＤ系ハードウエアの組み合わせに対してＥＭＤ系コンテンツを記録あるいは再生する場合、この場合は、本ＥＭＤシステムの典型的な流通形態であり、ＥＭＤシステムの権利処理ルールに従って、記録および再生とも可能である。

【００５５】次に、ＥＭＤ系メディアとＳＣＭＳ系ハードウエアの組み合わせに対して、ＳＣＭＳ系コンテンツを記録あるいは再生する場合、この場合は、単にＥＭＤ系メディアをＳＣＭＳ系メディアとして扱えばよい訳なので、技術的にも記録／再生可能であり、また、メディアの互換性という観点からも、記録／再生可能とするべきである。また、ＥＭＤ系メディアとＥＭＤ系ハードウ

17

エアの組み合わせに対してＳＣＭＳ系コンテンツを記録および再生する場合、この場合も、ＥＭＤ系ハードウエアにおいてＥＭＤ系メディアをＳＣＭＳ系メディアとして扱えばよい訳なので、技術的にも記録／再生可能であり、また、前のケースと同様に、メディアの互換性という観点からも記録／再生可能とするべきである。

【００５６】このような利用空間調査を行なうために、ＥＭＤシステム１においては、次のような構成を用いている。まず、表１に示したような記録／再生可能な条件を設定することにより、ＥＭＤ系ハードウエアにおいては、ＥＭＤ系メディアがセットされた場合に、そのＥＭＤ系メディアがＥＭＤ系メディアとして使用されている場合とＳＣＭＳ系メディアとして使用されている場合とがあることになる。そこで、図８を参照して前述したように、ＥＭＤ系メディアには、使用形態、すなわち、ＥＭＤ系メディアとして使用するのかＳＣＭＳ系メディアとして使用するのかを示すマニュアルスイッチ１２７を具備し、ＥＭＤ系ハードウエアにおいては、ＥＭＤ系メディア検出器５２４によりこれを検出するようにしている。

【００５７】また、ＥＭＤ系メディアに記録されているコンテンツは、ＥＭＤ系ハードウエアで記録された場合には暗号化されたＥＭＤ系コンテンツとして記録され、ＳＣＭＳ系ハードウエアで記録された場合には暗号化されていないＳＣＭＳ系コンテンツとして記録されている。すなわち、１つのＥＭＤ系メディアには、異なる形態のコンテンツが混在して記録されていることになる。したがって、再生する場合には、その記録形態を判別する必要がある。そこで、ＥＭＤシステム１においては、コンテンツの形態は各ＥＭＤ系メディアのＴＯＣに記録しておくようにしている。具体的には、ＴＯＣに、ＳＣＭＳ系コンテンツであれば０、ＥＭＤ系コンテンツであれば１となるようなフラグを設けている。これにより、ＥＭＤ系ハードウエアにおいては、ＴＯＣ情報に応じてシステムを切り換えるようにすれば、適切に再生が行なえる。

【００５８】２．所有権の調査

ＥＭＤシステム１においては、物理的にはコピー可能な場合であっても、権利処理の関係から、コピーを不可能にしたり、課金処理を行なう場合などがある。具体的には、コンテンツデータのコピーに関しては、コピーフリーの私的録音か課金処理を行なう個人間売買かを判別する必要がある。そこで、記録メディアおよびハードウエアの所有者を調査し、たとえば、他人のハードウエアに自分の記録メディアを搭載しているなどという状態を検出する。そして、これに基づいてコピーの制限や、課金処理を行なう。

【００５９】３．権利分配のための利用空間調査

ＥＭＤシステム１においては、コンテンツデータの配信により得られた利益は、最終的にＥＭＤサービスセンタ

18

１００において、その配信に係わった関係者に所定の比率で分配されるようになっている。そして、その関係者としては、たとえば機器製造者や、圧縮符号化方式など特定の処理の権利者なども含まれる。したがって、権利分配の観点から、それら関係者は全て調査して把握しておく。

【００６０】４．フォーマット変換係数に関する利用空間調査

ＥＭＤシステム１においては、種々の信号諸元のコンテンツデータを扱っている関係上、コピーなどを行なう場合にはレート変換などの信号諸元の変換が必要となる場合がある。そして、課金処理を行なう場合には、このような変換に基づく信号の劣化などを考慮する必要がある。すなわち、品質の劣化を伴うコピーは安価にし、高い品質でコピーされる場合は高い価格を設定するのが望ましい。そこで、コピー時などに、これら信号諸元を調査しておき、課金処理時に考慮する。また、この信号諸元の変換に係わる調査は、実際に信号の変換を行なう処理の制御にも必要である。

【００６１】利用空間調査手順

そして、たとえば図１７に示したようなコピーを行なう場合には、次のような手順で利用空間調査を行なう。まず、再生側において、メディアとハードウエア間の利用空間の調査を行なう。そのため、まず再生側の記録メディアのメディアＳＡＭが再生機器に対して自分の素性を送る。次に、再生機器においては、ＳＡＭに利用空間ディスクリプタを生成し、再生側の機器のＳＡＭに記述されているその機器の扱える信号処理などの利用空間のデータを、利用空間ディスクリプタにセットする。

【００６２】次に、その利用空間ディスクリプタに、メディアの情報をセットする。すなわち、メディアとハードウエアの間で相互認証を行なって、両サイドでセッション鍵を保有し、メディアＳＡＭの中に記述されているセキュアデータを全て、ハードウエアのＳＡＭに転送する。これにより、再生側の利用空間調査は終了する。次に、記録側においても、記録機器と記録メディアの間で、同様の利用空間調査を行なう。そして、最後に、記録機側の利用空間調査結果を再生側に送ることにより、再生側の機器のＳＡＭに、利用空間ディスクリプタが完成する。このようにして生成される利用空間ディスクリプタ（利用空間テーブルとも言う。）を図１８に示す。

【００６３】なお、ここでは再生側と記録側が１対１の場合を示したが、再生側１に対して、複数の記録機器に対してコピーを行なう場合もある。このような場合には、各々図１８に示したのと同様の情報で構成される、図１９に示すような、利用空間調査テーブルを生成する。

【００６４】ホームネットワーク機器の動作

次に、前述したような本発明に係わるユーザホームネットワーク４００の各機器において、たとえば図１７に示

したようなパッケージメディアからパケージメディアへ音楽データを複写する際の前述した利用空間調査の処理を含む動作について、図２０～図２７のフローチャートを参照して説明する。なお、実際にコンテンツデータのコピーを開始した以降は、既存の通常の機器の処理と同じであるので、ここでは、実際のコピー動作以前の初期動作を中心に説明する。

【００６５】まず、この初期動作の処理の全体の流れについて、図２０のフローチャートを参照して説明する。まず最初に、搭載された記録媒体の種別判別を行い（ステップＳ１１）、搭載されている記録媒体がＥＭＤ系メディアであった場合には（ステップＳ１２）、さらにそのメディアがＳＡＭを有し自らストレージ鍵を生成することのできるアクティブなメディアであるか否かを検査する（ステップＳ１３）。記録メディアが、ＳＡＭを有していないメディアであった場合には。ドライブＬＳＩ５２８でストレージ鍵を生成しておく（ステップＳ１４）。

【００６６】次に、記録メディアがアクティブメディアの場合には公開鍵方式により、また、記録メディアがポジティブメディアの場合には共通鍵方式により、記録メディアとドライブＣＰＵ５２０との間で相互認証を行なう（ステップＳ１５）。（以後の説明は、記録メディアがアクティブメディア７１０であるとして説明を行なう。）

次に、記録メディアに記録されているリボケーションリストを更新する処理を行い（ステップＳ１６）、更新が終了したら、まずメディアＳＡＭ６１０からＳＡＭ６００の対してのリヴォケーションチェックを行い、次にＳＡＭ６００～メディアＳＡＭ６１０へのリヴォケーションチェックを行なう（ステップＳ１７）。

【００６７】そして、鍵データブロックの物理アドレス情報のＳＡＭへの転送および設置処理を行い（ステップＳ１８）、さらに、鍵データブロックのＳＡＭ６００およびＡＶ圧縮伸張部への転送処理を行い（ステップＳ１９）、最後にファイルシステムをシステムメモリ５１２に転送する処理を行い（ステップＳ２０）、利用空間調査を含む、コンテンツデータの転送以前の一連おん初期処理を終了する（ステップＳ２１）。以後、各処理について詳細に説明する。

【００６８】まず、ステップＳ１１の、記録メディアの種別判別の処理について図２２のフローチャートを参照して説明する。まず、たとえばメディア検出スイッチ５２６が記録メディア７１０の挿入を見地するなどして処理を開始したら（ステップＳ３０）、メディア検出スイッチ５２６はこれをドライブＣＰＵ５２０に通知する（ステップＳ３１）。また、ＥＭＤ系メディア検出器５２４においては、記録メディア７１０のマニュアルスイッチ７１２に状態が検出され（ステップＳ３２）、記録メディア７１０の判別結果がドライブＣＰＵ５２０に通知される（ステップＳ３３）。

【００６９】そして、記録メディア７１０がＥＭＤ系メディアであった場合には（ステップＳ３４）、ドライブＣＰＵ５２０が、メディアＳＡＭＩ／Ｆ５２２を介して記録メディア７１０のメディアＳＡＭ６１０に対して、乱数生成を要求する（ステップＳ３５）。これにより、もし記録メディア７１０がメディアＳＡＭ６１０を有するアクティブな記録メディアであった場合には、メディアＳＡＭ６１０で乱数が生成され（ステップＳ６７）、生成した乱数がメディアＳＡＭＩ／Ｆ５２２を介してレジスタに格納され（ステップＳ３７）、メディアＳＡＭＩ／Ｆ５２２からドライブＣＰＵ５２０に乱数が格納された旨が通知される（ステップＳ３８）。すなわち、これらの動作の有無により、ドライブＣＰＵ５２０は記録メディアがアクティブメディアかポジティブメェイアかを判別することができる（ステップＳ３９）。

【００７０】そして、ドライブＣＰＵ５２０がホストＣＰＵ５１０に、搭載して記録メディアの種別を通知し（ステップＳ４０）、同時にＳＡＭ６００も、記録メディアの種別情報をスタックし（ステップＳ４１）、記録メディアの種別判別処理が終了する（ステップＳ４２）。

【００７１】次に、ステップＳ１５の、相互認証処理について、図２２のフローチャートを参照して説明する。まず、処理がスタートしたら（ステップＳ９０）、ホストＣＰＵ５１０が、ＳＡＭ６００に対して、記録メディア７１０と相互認証を行なうようにファンクションコールを送る（ステップＳ９１）。これに基づいて、メディアＳＡＭ６１０とＳＡＭ６００との間で、公開鍵暗号をベースとした相互認証を行なう（ステップＳ９２）。そして、ＳＡＭ６００はＳＡＭ６００に対して結果を通知し（ステップＳ９３）、相互認証処理は終了する（ステップＳ９４）。

【００７２】次に、ステップＳ１６の、リヴォケーションリストの更新処理について図２３のフローチャートを参照して説明する。まず、処理が開始されたら（ステップＳ５０）、メディアＳＡＭ６１０に格納されているリヴォケーションリストをストレージ鍵で復号する（ステップＳ５１）。次に、そのリヴォケーションリストを、ＳＡＭ６００の公開鍵で暗号化し（ステップＳ５２）、メディアＳＡＭＩ／Ｆ５２２、ドライブＣＰＵ５２０およびホストＣＰＵ５１０を介して、ＳＡＭ６００に転送してもらう（ステップＳ５３）。転送された、リヴォケーションリストは、ＳＡＭ６００内で、ＳＡＭ６００の秘密鍵を用いて復号化される（ステップＳ５４）。

【００７３】そして、ＳＡＭ６００に格納されているリヴォケーションリストを読み出し（ステップＳ５５）、ＭＡＣ鍵で復号してＳＡＭ６００内部に格納されているＭＡＣ値と比較し、改ざんがないことをチェックする（ステップＳ５６）。そして、記録メディア７１０から

読み出したリヴォケーションリストと、ＳＡＭ６００に格納していたリヴォケーションリストのヴァージョン番号を比較し（ステップＳ５７）、ＳＡＭ６００に格納していたリヴォケーションリストの方が新しければ（ステップＳ５８）、このリヴォケーションリストをメディアＳＡＭ６１０の公開鍵で暗号化し（ステップＳ５９）、ホストＣＰＵ５１０、ドライブＣＰＵ５２０およびメディアＳＡＭＩ／Ｆ５２２を経由してメディアＳＡＭ６１０に転送することにり（ステップＳ６０）、メディアＳＡＭ６１０のリヴォケーションリストを更新し、処理を終了する（ステップＳ６１）。

【００７４】次に、ステップＳ１７の、リヴォケーションリストのチェックの処理について、図２４のフローチャートを参照して説明する。まず、チェックの処理が開始されたら（ステップＳ７１）、メディアＳＡＭ６１０からＳＡＭ６００にコマンドを送ることにより（ステップＳ７２）、ＳＡＭ６００のＩＤがメディアＳＡＭ６１０に転送される（ステップＳ７３）。メディアＳＡＭ６１０は、このＩＤがリヴォケーションリストに含まれているか否かをチェックし、含まれていた場合には、このＳＡＭ６００を有する機器は、たとえば何らかの不正を行なうなど不適切な装置であると判定され、メディアＳＡＭ６１０は記録再生機器４１４との通信を拒絶し（ステップＳ７６）、処理を終了する（ステップＳ７７）。

【００７５】ＳＡＭ６００のＩＤがリヴォケーションリストに含まれていない場合には（ステップＳ７５）、次にＳＡＭ６００からメディアＳＡＭ６１０のチェックが開始され（ステップＳ７８）、ＳＡＭ６００からメディアＳＡＭ６１０にコマンドが送られて（ステップＳ７９）、メディアＳＡＭ６１０のＩＤがＳＡＭ６００に転送される（ステップＳ８０）。ＳＡＭ６００は、このＩＤがリヴォケションリストに含まれているか否かをチェックし、含まれていた場合には、この記録メディア７１０はたとえば何らかの不正が行なわれたなど不適切な記録メディア７１０であると判断し、以後の通信を拒絶し（ステップＳ８３）、処理を終了する。メディアＳＡＭ６１０のＩＤがリヴォケーションリストに含まれていない場合には（ステップＳ８２）、ＳＡＭ６００およびメディアＳＡＭ６１０とも適正なＳＡＭ、すなわち、記録再生機器４１４および記録メディア７１０はともに適正な装置および媒体であると判断され、一連のチェック処理は終了する（ステップＳ８５）。

【００７６】次に、ステップＳ１８の、鍵データブロックの物理アドレス情報の上位への転送処理について、図２５のフローチャートを参照して説明する。まず、処理がスタートすると（ステップＳ１００）、鍵データブロックの物理アドレスの情報をストレージ鍵で復号し（ステップＳ１０１）、鍵データブロックの物理アドレス情報をメディアＳＡＭ６１０の公開鍵で暗号化する（ステップＳ１０２）。そして、メディアＳＡＭ６１０は、この暗号化された情報を、メディアＳＡＭＩ／Ｆ５２２、ドライブＣＰＵ５２０およびホストＣＰＵ５１０を介して、ＳＡＭ６００に転送する（ステップＳ１０３）。

【００７７】ＳＡＭ６００では、鍵データブロックの物理アドレス情報全体のハッシュ値をとり、データ全体が改ざんされていないかどうかのチェックを行い（ステップＳ１０４）、適正であればその物理アドレス情報をＳＡＭ６００内にセットする（ステップＳ１０５）。次に、ＡＶコーデックＳＡＭ６２０と共通鍵暗号をベースとした相互認証を行い（ステップＳ１０６）、セッション鍵を共有し（ステップＳ１０７）、鍵データブロック情報をＡＶコーデックＳＡＭ６２０に転送する（ステップＳ１０８）。ＡＶコーデックＳＡＭ６２０では、これをセッション鍵を用いて復号し（ステップＳ１０９）、鍵データをメモリに格納し（ステップＳ１１０）、一連の転送処理は終了する（ステップＳ１１１）。

【００７８】次に、ステップＳ１９の、鍵データブロックの上位への転送処理について、図２６のフローチャートを参照して説明する。まず、処理がスタートすると（ステップＳ１２０）、鍵データブロックをストレージ鍵で復号し（ステップＳ１２１）、鍵データブロックをメディアＳＡＭ６１０の公開鍵で暗号化する（ステップＳ１２２）。そして、メディアＳＡＭ６１０は、この暗号化された情報を、メディアＳＡＭＩ／Ｆ５２２、ドライブＣＰＵ５２０およびホストＣＰＵ５１０を介して、ＳＡＭ６００に転送する（ステップＳ１２３）。

【００７９】ＳＡＭ６００では、鍵データブロック全体のハッシュ値をとり、データ全体が改ざんされていないかどうかのチェックを行う（ステップＳ１２４）。そして、適正であれば、ＡＶコーデックＳＡＭ６２０と共通鍵暗号をベースとした相互認証を行い（ステップＳ１２５）、セッション鍵を共有し（ステップＳ１２６）、鍵データブロックをＡＶコーデックＳＡＭ６２０に転送する（ステップＳ１２７）。ＡＶコーデックＳＡＭ６２０では、これをセッション鍵を用いて復号し（ステップＳ１２８）、鍵データをメモリに格納し（ステップＳ１２９）、一連の転送処理は終了する（ステップＳ１３０）。

【００８０】そして最後に、ステップＳ２０で示した、ファイルシステムの上位への転送処理について、図２７のフローチャートを参照して説明する。まず、処理がスタートすると（ステップＳ１４０）、ドライブＣＰＵ５２０が記録メディア７１０上の物理アドレス情報を管理するコンテンツファイルのファイルシステムを検出して、記録メディア７１０より読み出す（ステップＳ１４１）。次に、ドライブＣＰＵ５２０は、このファイルシステムをホストＣＰＵ５１０に転送し（ステップＳ１４２）、ホストＣＰＵ５１０は、これをシステムメモリ５１２上に記憶し（ステップＳ１４３）、ファイルシステムの転送処理は終了する（ステップＳ１４４）。

【００８１】ＥＭＤシステム１の動作

最後に、このような利用空間調査を行なう前述したような構成のＥＭＤシステムにおける、音楽コンテンツの配信の動作、処理の流れについてまとめて説明する。

【００８２】情報配信

まず、音楽コンテンツデータの配信処理の流れについて、典型的な一例を挙げて今一度まとめて説明する。まず、図１に示すようなＥＭＤシステム１において、コンテンツプロバイダ２００で著作権者により管理されている音楽コンテンツデータは、図２に示したコンテンツプロバイダセキュアコンテナの形態でサービスプロバイダ２５０に供給される。サービスプロバイダ２５０は、その音楽コンテンツデータを、図３に示したサービスプロバイダセキュアコンテナの形態で、種々のサービス形態により、また種々のデリバリチャネル３００を介して、たとえば図４に示すような構成のユーザホームネットワーク４００に配信する。この際、いわゆるポータルといわれる業者などにより、そのコンテンツデータの一部が使用されて、音楽コンテンツの参照、紹介、批評あるいは新たな形態の間接的な販促活動などが行なわれる場合もある。

【００８３】このようにしてユーザホームネットワーク４００に配信された音楽コンテンツデータは、配信された直後は、通常は特段の処理が行なわれずに、サービスプロバイダセキュアコンテナの形態でそのまま家庭内のストレージ機器のハードディスクなどに記憶される。そして、使用者がこのサービスプロバイダセキュアコンテナに含まれる音楽データを再生したり記録する、すなわち使用すると決定し、たとえば家庭内の記録再生装置４１２において相応の操作を行った場合に、記録再生装置４１２内のＳＡＭが、サービスプロバイダセキュアコンテナ内の図６に示したようなＵＣＰを読み出し、ＵＣＰ内に設定されている取扱方針で許される範囲内での使用形態を決定し、使用状態を示すＵＣＳを生成し、図５に示すようなユーザホームネットワークセキュアコンテナが生成される。

【００８４】以後、家庭内の記録再生装置４１２において、ＥＭＤサービスセンタ１００より予め配布されているディストリビューション鍵を用いることにより、暗号化された音楽コンテンツデータが適宜復号されて再生されるなど使用される。また、このユーザホームネットワークセキュアコンテナの形態で、許される範囲内で順次コピーが行われる。

【００８５】ホームネットワーク機器の動作

ユーザホームネットワーク４００の各ホームネットワーク機器間におけるデータの流れ、および、データ配信状態について図２８～図４２の各具体例を参照して説明する。

【００８６】まず、図２８に、機器のホストＣＰＵ５００とＳＡＭ６００およびメディア７１０との関係を示す。前述したように、ＳＡＭ６００は、ホストに対してＩ／Ｏとして接続されており、Ｉ／Ｏ命令により制御される。ホストＣＰＵ５００に対しては、ＳＡＭ６００はスレーブ、ＳＡＭ６００とメディア７１０との間では、ＳＡＭがマスタ、メディアがスレーブとなる。メディア７１０はＳＡＭ６００に接続されており、ファンクションコールおよびリザルトにより処理を進める。ファンクションコールはコマンドとコンテンツを特定するための番号を含む情報である。キーファイルは、メディアとＳＡＭとで処理し、コンテンツファイルは、ＳＡＭが処理する場合もあるし、ホストＣＰＵが記録する場合もある。ファイルシステムは、キーファイルのファイルシステムはＳＡＭに展開し、コンテンツファイルのファイルシステムはホストＣＰＵに展開する。

【００８７】図２９は、ＡＶコーデックを有する機器における、ホストＣＰＵ、ＳＡＭ、ＡＶコーデックＳＡＭおよびメディアとの関係を示す図である。この形態の機器では、メディアを挿入した時点で、キーファイルはまとめてＳＡＭに展開し、新たに加わったキーデータも含めて、イジェクト時にまとめてメディアに転送する。この場合は、メディアＳＡＭとＳＡＭとの間で、公開鍵方式により相互認証を行なってセッションキーを生成し、セッションを行なって、キーファイルとキーファイルＴＯＣとをＳＡＭ側にストックする。

【００８８】コンテンツファイルは、ホストＣＰＵ側にファイルシステムを送る。これによりホストＣＰＵがファイルシステムを読んで、特定のコンテンツファイルをコーデックＳＡＭに送るように命令すると、ＳＡＭとＡＶコーデックＳＡＭとがトリプルＤＥＳによる相互認証を行なってセッションキーを生成し、これにより所望のコンテンツ、たとえば、コンテンツ１、４、５のコンテンツキーをＳＡＭからＡＶコーデックＳＡＭに転送する。また、アナログ出力のためのウォーターマークデータも、セッションキーにより暗号化してＡＶコーデックＳＡＭに転送する。これにより、メエィアから再生した圧縮データを、ＡＶコーデックＳＡＭでリアルタイムに復号化し、ウォーターマークを付加して出力する。

【００８９】図３０は、ハードディスクに暗号化されたコンテンスファイルがＣＡを介して、ダウンロードされてきて、これを試聴してみて、再生してみて、利用形態を決定するというプロセスを説明するための図である。この装置においては、コンディショナルアクセス（ＣＡ）が、デリバリーサービスより、たとえばＣＦ－１～ＣＦ－２０の２０個のコンテンツファイルをダウンロードしてくる。そして、コンテンツファイルはＡＶ－ハードディスク５３０に、キーファイルは、ＳＡＭにより管理されるＥＥＰＲＯＭ５１４にロードされる。ＳＡＭとＡＶコーデックＳＡＭでトリプルＤＥＳで相互認証を行い、再生したいコンテンツのキーファイルをＡＶコーデックＳＡＭに送り、ＡＶコーデックで再生出力する。

25

【００９０】ホストＣＰＵは、ＳＡＭに対してＩ／Ｏリードライトでファンクションコールを送ってリザルトをもらう。また、ＨＤＤに対してもＩ／Ｏリードライトで指令をして、たとえばコンテンツ７を読み出しＡＶコーデックに出力させる。ＳＡＭは、メモリリードライトによりファイルシステムに基づいて、ファイルシステムをスタックして、コンテンツキーＡＶコーデックに送る。ＧＵＩでボタンを押された、ホストに割り込みが入って、ダウンロードが開始される。ダウンロードが開始されたら、ホストはＳＡＭにお願いし、キーファイルを格納させる。

【００９１】図３１は、ハードディスクの中にセキュア領域がある場合である。この場合は、ハードディスクの中にキーファイルを入れてしまい、ＨＤＤは、ホストとＳＡＭの共有記憶空間になる。ＨＤＤに記憶されているキーファイルにはＳＡＭのみがアクセス可能である。鍵ファイルのファイルシステムはサムがスタックし、コンテンツファイルのファイルシステムは、ホストＣＰＵがスタックする。

【００９２】図３２は、ネットワーク機器の中にパッケージメディアが入っている場合の構成を示す。この場合は、サムとメディアＳＡＭが相互認証を行い、キーファイルをセッションキでメディアＳＡＭに送る。そして、メディアＳＡＭ側で、セッションキーを解いて、ストレージキにより暗号化し、鍵のかけかえを行ない、メディアＳＡＭに記録する。サムは、ホストにＯＫを返答し、ホストはＩ／Ｏリードライトで、コンテンツファイルをメディアに記録する。この時に、利用空間を調査し、必要であれば、諸元変換を行なってから記録する。

【００９３】図３３は、図１７に示したのと同様の、ＥＭＤシステム１における典型的な複写処理の例である。この構成では、ネットワーク機器と別にパッケージ機器があって、物理的な線でつないでダウンロードする。したがって、ＳＡＭ－ＳＡＭ間の認証が必要となる。認証は、両機器のホストとＳＡＭ間と、ＳＡＭ－ＳＡＭ間で行なわれる。再生側は、キーファイルをメモリから取り出して、ＳＡＭ－ＳＡＭ間で相互認証を行いセッションキーをつくって、キーファイルを記録側に送る。記録側では、メディアＳＡＭと相互認証を行なってメディアのキーファイルを展開する。

【００９４】購入形態は、送り側で決めてもよいし、記録側で決めてもよい。利用空間調査は、両サイドの機器で行なう。再生側のホストＣＰＵが持っているのはハードディスクに記録されているコンテンツファイルのファイルシステムであり、ＳＡＭの持っているキーファイルのファイルシステムは、メモリに記録されているキーファイルのファイルシステムである。記録側のホストＣＰＵが持っているのはパッケージメディアに記録されているコンテンツファイルのファイルシステムであり、ＳＡＭに持っているキーファキルおよびファイルシステム

26

は、パッケージメディアのものである。

【００９５】図３４は、パッケージ間の再配付の場合を示す図である。再生の機器とメディアで利用空間調査を行い、ＳＡＭと記録系でメディア空間を行い、キーファイルはＳＡＭに展開して、コンテンツファイルはＨＤＤ上に展開する。利用形態は、ＵＣＰを移すのみ。したがって、セッションキーをつくって、ＵＣＰ、キーファイルのみを転送し、コンテンツファイルはそのまま転送する。ＳＡＭとメディアＳＡＭで相互認証し、キーファイルを送り、コンテンツファイルはメディアに記録する。再生側でＵＣＳを作り、購入形態を決める。記録側に転送する時は、ＫＦ１－ＵＣＰだが、メディアに記録される時には、ＫＦ１－ＵＣＰ／ＵＣＳとなっている。なおこの場合、利用空間調査で諸元が同じことがわかっているものとする。

【００９６】図３５は、諸元が違う場合の例である。再配付だけど諸元が違う。この利用空間では、再生側に変換処理を持っているので、コンテンツはコンテンツキーで復号し、コンテンツキーを記録側にセッションキーで送る。そして、信号を変換して、セッションキーで送って、記録側にスタックしているコンテンツキーで再暗号化してメディアに記録する。再暗号化はドライブで行なう。ドライブにＤＥＳがあるので、ここで暗号化しながら記録する。

【００９７】図３６は、ＵＣＳからの購入の例を示す図である。再生課金の場合を示し、利用空間調査と、キーファイル展開の操作は前述した場合と同じである。この場合、諸元は同じであり、セッションキーは、ＳＡＭ－ＳＡＭ間、ＳＡＭ－メディアＳＡＭ間で持っている。また、ＵＣＳのキーファイルをセションキーで送る。

【００９８】図３７は、買い切りの場合である。利用空間調査の中に、誰が購入したか。また、記録媒体は誰のものという判別により、私的録音、プライベートユーセージ／セルの区別をつける。所有権の利用空間調査も必要である。ＵＣＳに記録されている所有者から、その記録媒体の所有者が同じなら移る。そうでない場合は課金される。

【００９９】図３８は、ＥＭＤからＳＣＭＳコンテンツへのコピーを示す。利用空間調査で相手がＳＣＭＳとわかるので、ＳＡＭで課金を行い、コンテンツキーで暗号化をはずしながら、１３９４コピープロテクションのセッションキーを使って、ホスＣＰＵ２に送って、メディアに記録する。この時のプロテクトモードは、コピー付加である。

【０１００】図３９は、利用空間調査でＳＡＭ機器にＳＣＭＳ機器が乗っている場合である。ＥＭＤ機器同志のセッションであるが、記憶側に載っているメディアがＳＣＭＳメディアなので、ＵＣＰに書かれているＥＭＤモードと諸元、および、相手の記録媒体のＳＣＭＳということで処理を行なう。この場合は、ＵＣＰに書かれてい

るＳＣＭＳメディアへの記録という報告を見て、１回当たりのコピーの価格をみて、これを再生側のＥＭＤ機器で支払う。再生側でコンテンツ鍵ではずして、セッション鍵で転送して記録してもいいが、記録側で記録するようにしてもよい。

【０１０１】図４０は、再生側がＳＡＭ機器で、ＳＡＭメディアだが、マニュアルスイッチによりＳＣＭＳメディアとして使用され、ＳＣＭＳコンテンツが搭載されている場合である。この例では、ＳＡＭ機器で、ＥＭＤメディアでＥＭＤモードで使用している機器にコピーを行なう。この場合、ＴＯＣ情報によりＳＣＭＳコンテンツであることがわかっているので、ＳＣＭＳコンテンツとして処理を行なう。送る時は、ＳＡＭ－ＳＡＭで相互認証して、セッションキーを作って、ＳＣＭＳコンテンツは、セッション鍵で暗号化して記録側に送り、記録側ではセション鍵を用いてはずす。そして、記録側で、コンテンツ鍵を生成して、これで暗号化して、メディアに記録する。最後に、生成したコンテンツキーをメディアＳＡＭに送って、セッション鍵をストレージ鍵で鍵をかけなおし保存する。

【０１０２】図４１は、シングルドライブコピーを示す。この場合、まず、ＲＯＭを入れ、キーファイルはＳＡＭ１に転送しファイルシステムを展開する。コンテンツファイルは、共有メモリ空間におく。次に、ＲＯＭディスクをはずす。ＲＡＭディスクをセットする。そして、ＳＡＭ１で購入形態処理を決定した上で、決定した鍵ファイル（ＵＣＳ鍵ファイル）および、商品そのもののＵＣＰ鍵ファイルをＲＡＭのメディアＳＡＭに記録する。最後に、コンテンツをＲＡＭに記録する。このようにすれば、デッキは２台必要なく、シングルのデッキでコピーできる。

【０１０３】図４２は、ＲＯＭディスクでの購入形態を示す。ＲＯＭを買った時は、購入形態がきまっていない。また、ＲＯＭ－ＲＡＭのハイブリッドが必要となる。この場合、メディアＳＡＭにあるキーファイルを全部ＳＡＭ１に転送し、試聴して、購入するコンテンツを選択する。そして、ＵＣＳキーファイルを作り、メディアＳＡＭに記録する。これにより、買った曲だけが聞けるＲＯＭディスクになる。ＲＡＭは、セキュアＲＡＭのみの場合、セキュアＲＡＭとメディアＳＡＭがある場合、セキュアＲＡＭがなくて全部メディアＳＡＭでやってしまう場合がある。

【０１０４】使用履歴情報

そして、このような種々の形態により、音楽コンテンツが課金される形態で実際に使用されるごとに、使用履歴情報（Usage-Log）が生成される。生成された使用履歴情報（Usage-Log）は、各ユーザホームネットワーク４００内のネットワーク機器４１０に一旦蓄積された後、適宜ＥＭＤサービスセンタ１００に送信される。

【０１０５】この使用履歴情報（Usage-Log）の一例を図

４３に示す。使用履歴情報（Usage-Log）には、図４３に示すように、コンテンツＩＤ（Content ID）、コンテンツを使用した利用者ＩＤ（User ID）、ユーザホームネットワーク４００を特定するホームネットワークグループＩＤ（Home Network Group ID）、権利処理を行なったＳＡＭのＩＤ（SAM ID）、購入形態を示す情報（Purchase/Usage mode）、価格（Price Tag）、使用地域（area-code）、割引情報（discount information）、そのコンテンツの販売に係わった全てのエンティティのＩＤ、使用の際の信号諸元の情報などが記録されている。エンティティとしては、コンテンツプロバイダ（Content Provider）、サービスプロバイダ（Service Provider）を初めとして、ポータル（E.M.Place）、ハードウェア提供元（H/W Provider）、記録媒体提供元（Media Provider）、装置製造元（Component Provider）、権利者（LicenceHolders）など、そのコンテンツの配信に係わった全てのエンティティが記録される。

【０１０６】利益分配処理

さて、このようなＥＭＤシステム１、またユーザホームネットワーク４００における音楽コンテンツデータの配信環境において、最終的に音楽コンテンツデータの購入に基づく利益を分配する方法について図４４～図４６を参照して説明する。なお、ここで言う利益とは、音楽コンテンツの配信に伴って得られる金銭的な価値を広く総称したものであって、実際の適用時には、購入金額、対価をそのまま用いてよい。図４４は、利益分配処理の流れを示すブロック図であり、図４５は、図４４に示した利益分配率データを説明するための図であり、図４６は、図４４に示した利益分配処理を説明するための図である。

【０１０７】前述したように、まず、ＥＭＤサービスセンタ１００には、図４４に示すように、基本的にＥＭＤシステム１の全てのエンティティが登録されており、ＩＤ、種々の属性、決済口座などの情報を含むエンティティ管理データ１１０が記録されている。また、図４５に示すような、各コンテンツプロバイダ２００から登録された、各コンテンツＩＤごと、すなわち、コンテンツプロバイダセキュアコンテナごとの、各エンティティに対する利益分配の割合を示した利益分配率データ１１２が記録されている。さらに、図示しないが、各コンテンツプロバイダ２００から登録された、各コンテンツデータの配信の際の信号諸元に基づいた価格変更、価格換算を規定した価格換算データ１１４が記録されている。

【０１０８】このような状況において、音楽コンテンツデータが購入されたら、前述したような各機器のＳＡＭあるいはメディアＳＡＭにおけるセキュアな処理により利用空間調査が行なわれ、最終的に、コンテンツの生成から購入に関わった全てのエンティティ、購入条件、信号諸元などが記録された、図４３に示したような使用履歴情報（Usage-Log）がＥＭＤサービスセンタ１００に送

29

信されてくる。

【０１０９】この使用履歴情報（Usage-Log）を、ＥＭＤサービスセンタ１００のたとえば利益分配サーバ１２０が受信したら、まず、最終的な購入価格を決定する。購入価格は、まず基本的に、買い切り（Sell Through）の場合は使用履歴情報（Usage-Log）に記載されているプライスタグが基準となり、また再生課金（Pay PerPlay）による購入の場合には１回の再生価格×使用履歴情報（Usage-Log）の個数が基準となる。そして、この基準価格に、さらに種々の条件に基づいて補正を行ない、最終的な購入価格を決定する。

【０１１０】具体的には、まず、使用履歴情報（Usage-Log）に記載されている購入時の信号諸元のデータに基づいて、価格換算データ１１４を参照して換算を行なう。たとえば、プライスタグが１ビット２．２８２２４ＭＨｚのサンプリングデータを基準としたものである場合に、これを１６ビット４４．１ＫＨｚＡＴＲＡＣ（登録商標）２にダウンサンプリングして購入した場合には、価格換算データ１１４を参照して、品質相応の換算を行なう。次に、使用履歴情報（Usage-Log）の使用地域の情報に基づいて、使用した国に応じて異なるたとえば付加金などの価格を検出し、この調整を行なう。さらに、たとえばマイレージなどのディスカウントを利用しているか否かなどの条件を加味し、最終的な価格を決定する。

【０１１１】一方で利益分配サーバ１２０は、使用履歴情報（Usage-Log）に記載されているコンテンツＩＤに基づいて、コンテンツデータごとの利益分配率データ１１２を参照し、そのコンテンツに関わる各エンティティに対する利益の分配率を決定する。また、使用履歴情報（Usage-Log）に記載されている各エンティティのＩＤに基づいて、エンティティ管理データ１１０を参照して、利益振込口座の口座番号を検出する。最後に、たとえば著作権利者にのみ付加される著作権料（copyright fee）のような料金の調整を行い、最終的に各エンティティに支払う価格を決定する。

【０１１２】支払い価格が決定されたら、たとえばＥＭＤサービスセンタ１００内の支払いサーバ１３０にそのデータを転送し、支払いサーバ１３０が、たとえば特定の期間ごとの決済処理を一括するなどした上で、カード会社や銀行などの決済機関８００を介して支払い処理を行なう。

【０１１３】このようにすることで、コンテンツデータを配信した、あるいは使用されたことによる対価を、必要に応じて媒体メーカや装置メーカも含めた、そのコンテンツデータの配信に関わった全てのエンティティに対して、そもそもコンテンツデータを生成したコンテンツプロバイダ２００が意図し設定した分配比率に従って、また、コンテンツデータの品質、購入形態、使用環境による制約などにも適切に対応した形態で、適切に配分することができる。

30

【０１１４】変形例

なお、本発明は本実施の形態に限られるものではなく、任意好適な種々の改変が可能である。たとえば、本実施の形態においては音楽データの配信システムを例示したが、静止画像データ、動画像（映像）データ、ビデオデータ、あるいは、コンピュータプログラムやゲームプログラム、ゲームの追加データなど、任意のデータの配信システムに適用可能である。

【０１１５】また、本実施の形態においては図１に示したような構成のＥＭＤシステム１を例示して本発明を説明したが、このような構成のシステムにのみ適用可能なものではない。たとえば、ＥＭＤサービスセンタ１００が存在せず、コンテンツプロバイダ２００自身が、エンティティ管理データ１１０、利益分配率データ１１２および価格換算データ１１４などを管理しておき、使用履歴情報（Usage-Log）を受け付けて、対価配分処理を行なうようにしてもよい。もちろん、これがサービスプロバイダ２５０や、ＥＭＤサービスセンタ１００とは異なる第３の機関により行なわれるような構成でもよい。また、コンテンツデータの配信環境についても、任意の構成でよい。たとえば、サービスプロバイダ２５０が存在せずコンテンツプロバイダ２００が直接に配信する構成であってもよい。

【０１１６】また、ＥＭＤサービスセンタ１００、コンテンツプロバイダ２００、サービスプロバイダ２５０、デリバリチャネル３００、ユーザホームネットワーク４００の各構成は何ら限定されるものではなく、各々任意の構成でよい。

【０１１７】

【発明の効果】このように、本発明によれば、適切に権利処理を行いながら記録することのできるデータ記録装置を提供することができる。また記録された所望のデータを、適切に権利処理を行いながら再生することのできるデータ再生装置を提供することができる。また、所望のデータを、任意の信号諸元で任意の媒体、通信路、機器を介して任意の配信先に所定の権利処理を行いながら配信するためのデータ処理装置を提供することができる。さらに所望のデータを、適切に権利処理を行いながら記録および再生することのできるデータ記録媒体を提供することができる。

【図面の簡単な説明】

【図１】図１は、本発明の一実施の形態のＥＭＤシステムの構成を示すブロック図である。

【図２】図２は、図１に示したＥＭＤシステムのコンテンツプロバイダが生成するコンテンツプロバイダセキュアコンテナを説明するための図である。

【図３】図３は、図１に示したＥＭＤシステムのサービスプロバイダが生成するサービスプロバイダセキュアコンテナを説明するための図である。

【図４】図４は、図１に示したＥＭＤシステムのユーザ

31

ホームネットワークの一般的な構成を示す図である。

【図５】図５は、図１に示したＥＭＤシステムのユーザホームネットワーク内で生成するユーザホームネットワークセキュアコンテナを説明するための図である。

【図６】図６は、ＵＣＰを説明するための図である。

【図７】図７は、ＵＣＳを説明するための図である。

【図８】図８は、ホームネットワーク機器の構成の第１の例を示す図である。

【図９】図９は、ホームネットワーク機器の構成の第２の例を示す図である。

【図１０】図１０は、ＳＡＭの構成の第１の例を示す図である。

【図１１】図１１は、ＳＡＭの構成の第２の例を示す図である。

【図１２】図１２は、ＡＶコーデックＳＡＭの構成を示す図である。

【図１３】図１３は、ドライブＳＡＭの構成の第１の例を示す図である。

【図１４】図１４は、ドライブＳＡＭの構成の第２の例を示す図である。

【図１５】図１５は、メディアＳＡＭの構成の第１の例を示す図である。

【図１６】図１６は、メディアＳＡＭの構成の第２の例を示す図である。

【図１７】図１７は、利用空間調査の概念を説明する図である。

【図１８】図１８は、利用空間ディスクリプタ（利用空間テーブル）を説明するための図である。

【図１９】図１９は、１つの再生装置から複数の記録装置にコピーを行なう場合の利用空間調査を説明するための、利用空間調査テーブルを示す図である。

【図２０】図２０は、利用空間調査を含む一連の初期処理の流れを示すフローチャートである。

【図２１】図２１は、装着された記録メディアの種別判別処理の流れを示すフローチャートである。

【図２２】図２２は、相互認証処理の流れを示すフローチャートである。

【図２３】図２３は、リヴォケーションリスト更新処理の流れを示すフローチャートである。

【図２４】図２４は、リヴォケーションリストチェック処理の流れを示すフローチャートである。

【図２５】図２５は、鍵データブロックの物理アドレス情報の上位への転送処理の流れを示すフローチャートである。

【図２６】図２６は、鍵データブロックの上位への転送処理の流れを示すフローチャートである。

【図２７】図２７は、ファイルシステムの上位への転送処理の流れを示すフローチャートである。

【図２８】図２８に、ホームネットワーク機器のホストＣＰＵとＳＡＭおよびメディアの基本的構成を示す図である。

32

【図２９】図２９は、ＡＶコーデックを有する機器における、ホストＣＰＵ、ＳＡＭ、ＡＶコーデックＳＡＭおよびメディアとの関係を示す図である。

【図３０】図３０は、ハードディスクに暗号化されたコンテンツファイルをダウンロードし、試聴した上で利用形態を決定するという状態を示す図である。

【図３１】図３１は、ハードディスクの中にセキュア領域がある場合を示す図である。

【図３２】図３２は、ネットワーク機器の中にパッケージメディアが入っている場合を示す図である。

【図３３】図３３は、ＥＭＤシステムと同様の構成による複写処理を示す図である。

【図３４】図３４は、パッケージ間の再配付の場合を示す図である。

【図３５】図３５は、諸元が違う場合の再送付の例を示す図である。

【図３６】図３６は、ＵＣＳからの購入の例を示す図である。

【図３７】図３７は、買い切りの場合を示す図である。

【図３８】図３８は、ＥＭＤからＳＣＭＳコンテンツへのコピーを示す図である。

【図３９】図３９は、利用空間調査でＳＡＭ機器にＳＣＭＳ機器が乗っている場合を示す図である。

【図４０】図４０は、再生側がＳＡＭ機器でＳＡＭメディアだが、マニュアルスイッチによりＳＣＭＳメディアとして用いられている場合を示す図である。

【図４１】図４１は、シングルドライブコピーを示す図である。

【図４２】図４２は、ＲＯＭディスクでの購入形態を示す図である。

【図４３】図４３は、利用履歴情報（Ｕｓａｇｅ－Ｌｏｇ）の内容を説明するための図である。

【図４４】図４４は、図１に示したＥＭＤシステムにおける利益分配処理の流れを示すブロック図である。

【図４５】図４５は、図４４に示した利益分配率データを説明するための図である。

【図４６】図４６は、図４４に示した利益分配処理を説明するための図である。

【符号の説明】

１…ＥＭＤシステム、１００…ＥＭＤサービスセンタ、１１０…エンティティ管理データ、１１２…利益分配率データ、１１４…価格換算データ、１２０…利益分配サーバ、１３０…支払いサーバ、２００…コンテンツプロバイダ、２５０…サービスプロバイダ、３００…デリバリチャネル、４００…ユーザホームネットワーク、４１０…ネットワーク機器、４１２，４１４，４１６…記録再生機器、５００…ホストＣＰＵ、５１２…システムメモリ、５１４…フラッシュＥＥＰＲＯＭ、５１６…ホストＣＰＵバス、５２０…ドライブＣＰＵ、５２２…メデ

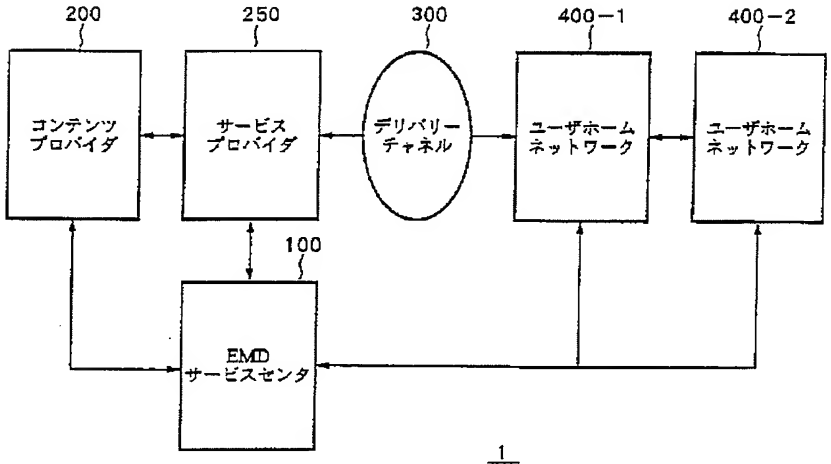
33

ィアＳＡＭインターフェイス、５２４…ＥＭＤ系メディア検出器、５２６…メディア検出スイッチ、６００…ＳＡＭ、６１０…メディアＳＡＭ、６２０…ＡＶコーデックＳＡＭ、６３０…ドライブＳＡＭ、７００…記録媒

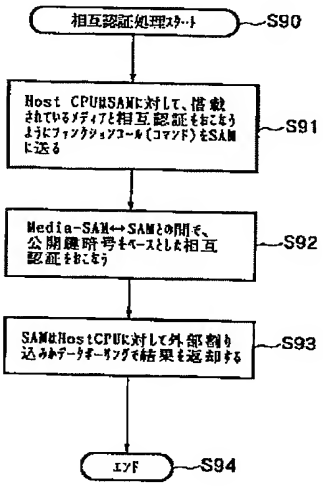
34

体、７１０…ＥＭＤ系メディア、７２０…ＳＣＭＳ系メディア、７２２…ＲＯＭ領域、７２４…セキュアＲＡＭ領域、７２６…ＲＡＭ領域、８００…決済機関

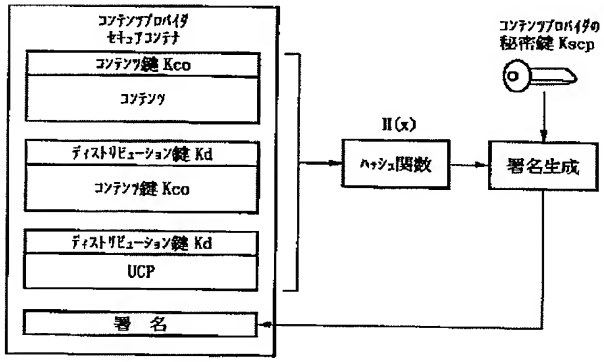
【図１】



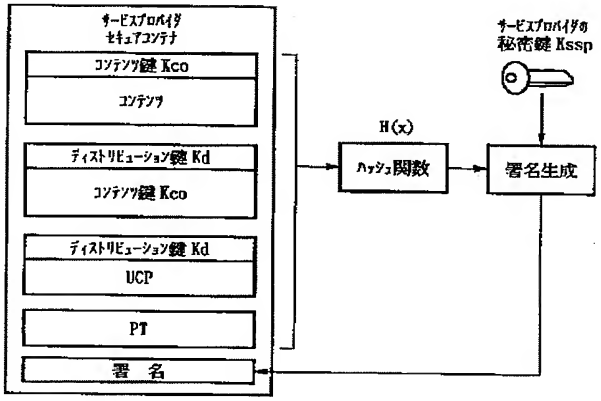
【図２２】



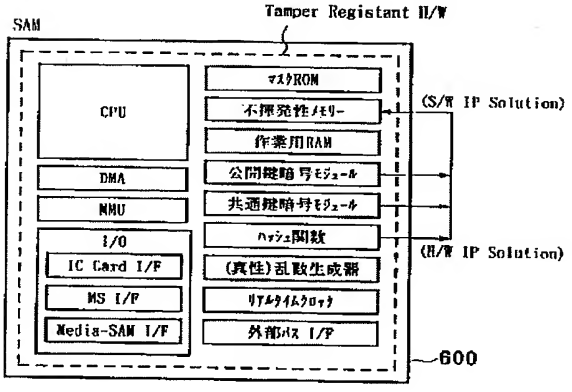
【図２】



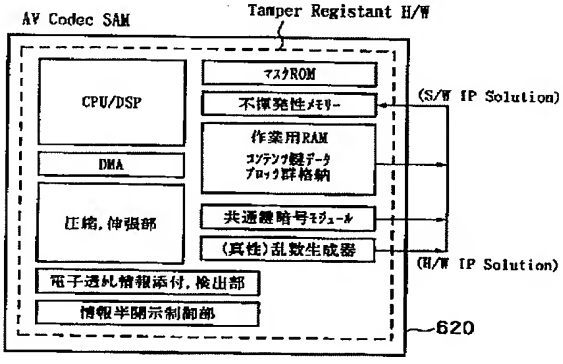
【図３】



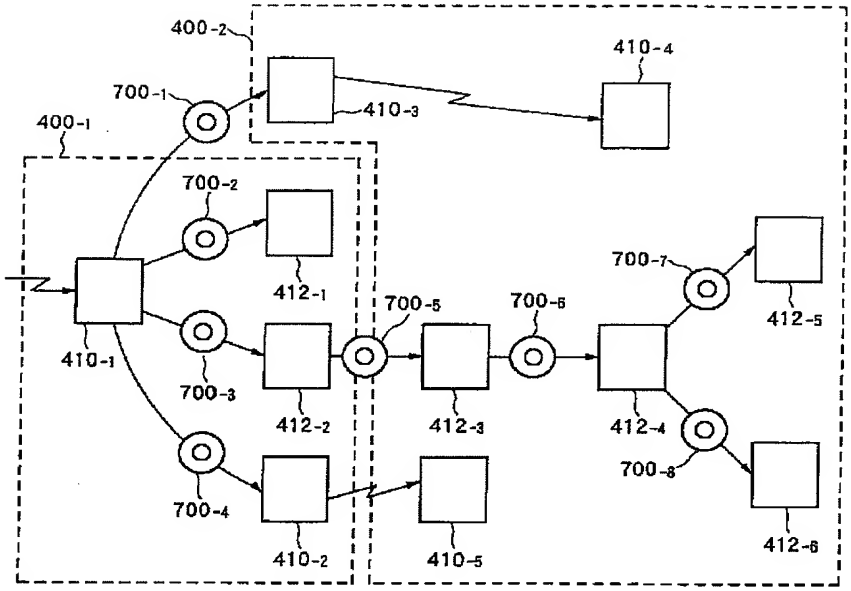
【図１０】



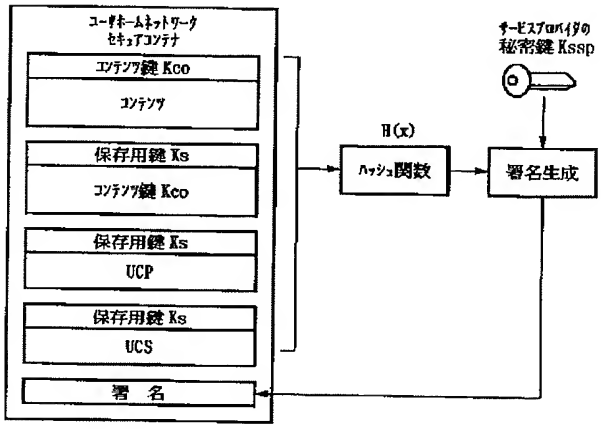
【図１２】



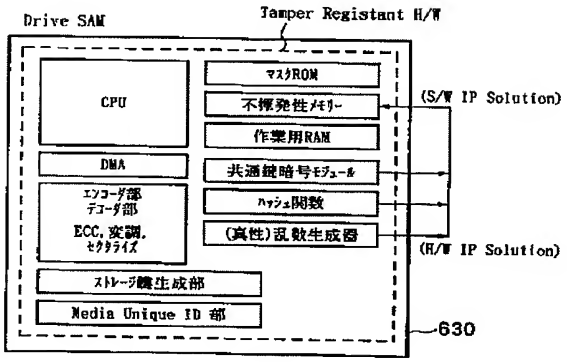
【図４】



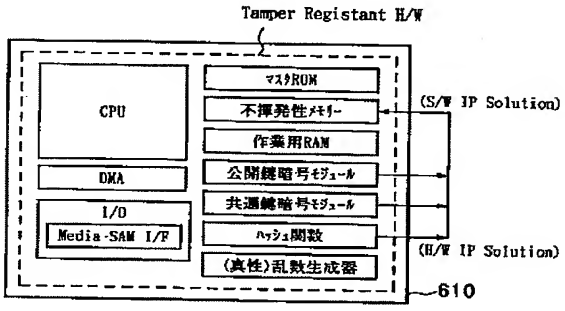
【図５】



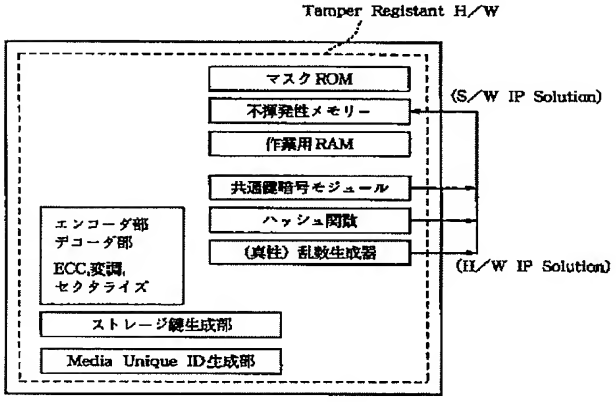
【図１３】



【図１５】



【図１４】



【図６】

Usage Control Policy(UCP)

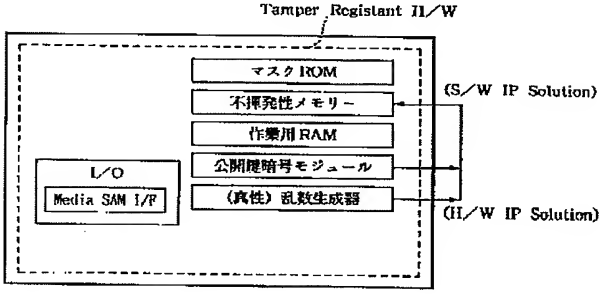
バージョン(Version NO.)
コンテンツプロバイダ アセットマネジメント管理用コンテンツID
署名(コンテンツプロバイダ秘密鍵)
第3信頼機関管理用グローバルユニークなコンテンツID
署名(第3信頼機関の秘密鍵)
国,エリアコード
作成者情報 Content Provider ID
作成年月日 Authoring Date
発行者情報:第3信頼機関情報
発行年月日 Issue Date
有効期限 Expiration Date(Validity)
第3信頼機関の通信アドレス
配信サービス事業者情報 Service Provider ID
コンテンツの種別情報① 映画/音楽/番組/CM/宣材
コンテンツの種別情報② 原作/2次利用/編集著作物
コンテンツの表現種別情報① 動画,静止画,音声他.
コンテンツの表現種別情報② 信号諸元,圧縮方式
利用空間調査による取扱制御情報
コンテンツプロバイダによるアクセス制御情報
ユーザによるアクセス制御情報(初期値)
マイレージ、割り引きクーポンに関する取扱方針
推薦決済手段 第3信頼機関/電子マネー決済
試聴デモサンプルの取扱制御情報(半開示パラメータ)
コンテンツ(商品)の販売機関/販売国,エリアコード
Usage Control
各購入形態における価格は、卸売価格
プロモーション用無料サービス期間/回数
再配付 Re-Distribution
再生課金 Pay-Per-Use　上限回数(-->Sell Through) 1回/2回/....n回の価格
買い切り Sell Through ①完全 ②期限制限 Time Limited ③回数制限 Pay Per Play N
買い切り Sell Through-SCMS
コピーフリー/コピー1回/コピー不可/コピー1回済
記録課金 Pay Per SCMS Copy N
コピーコントロールチケット 購入枚数
時間(毎)課金 Pay Per Time
ブロック単位課金 Pay Per Block
SCMS機器との互換性 ①EMD -->SCMS ②SCMS -->EMD

【図７】

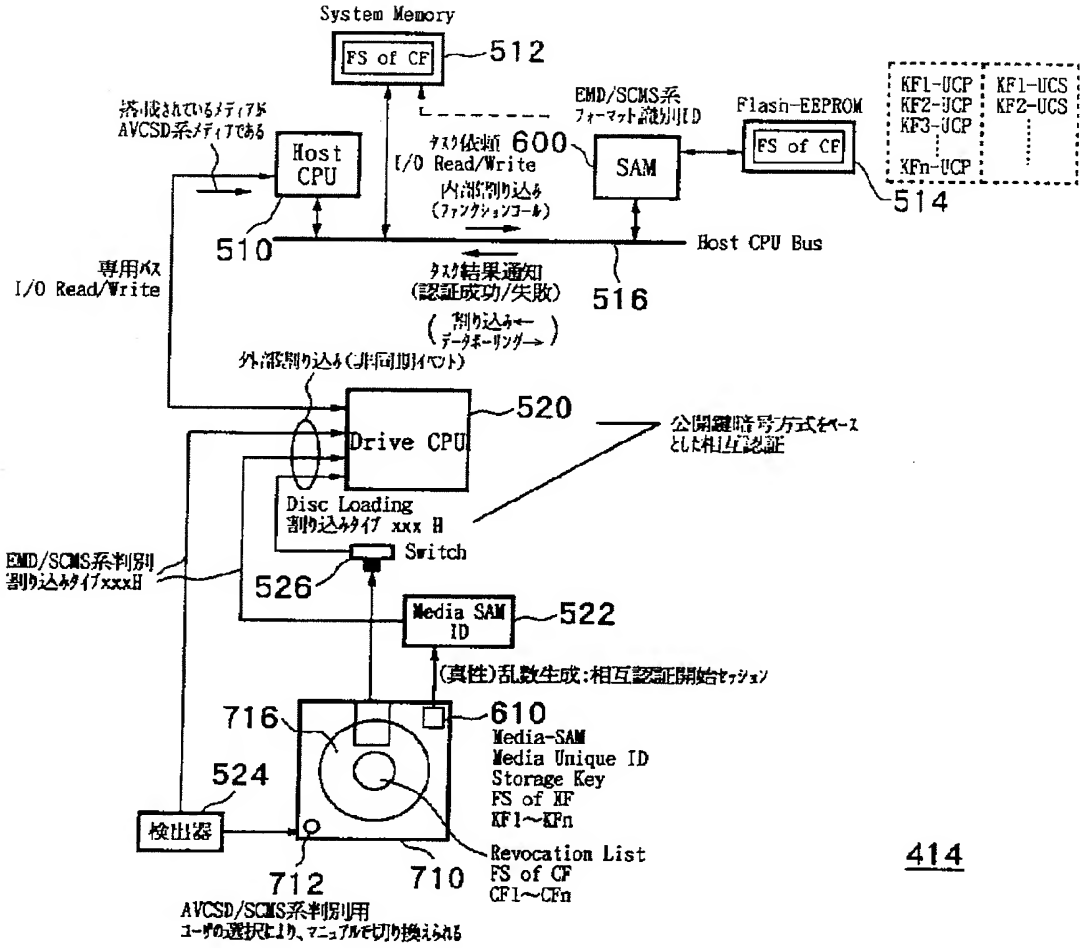
Usage Control Status(UCS)

コンテンツプロバイダ アセットマネジメント管理用コンテンツID CP_Content ID for Asset Management
署名(コンテンツプロバイダ秘密鍵)
第3信頼機関管理用グローバルユニークなコンテンツID CA_Content ID(Globally Unique)
署名(第3信頼機関の秘密鍵)
配信サービス事業者情報 Service Provider ID
配信サービス名
サービスプロバイダ配信サービス管理用コンテンツID SP_Content ID for Delivery Service
署名(サービスプロバイダ秘密鍵)
発行者情報 HNG-ID/SAM_ID/Media SAM_ID
購入者情報 UserID
購入者が選択した決済手段 第3信頼機関/転々流通(電子マネー)
購入者決済手段情報 ①銀行、登録講座 ②クレジットカード会社 ③クレジットカードナンバー
購入トレース情報 (1回目購入) 購入日付/購入者情報/発行者情報 購入機器情報/購入媒体情報 他 (2回目購入) 購入日付/購入者情報/発行者情報 購入機器情報/購入媒体情報 他 (n回目購入) 購入日付/購入者情報/発行者情報 購入機器情報/購入媒体情報 他
コンテンツ販売価格 PT(Price Tag)
購入、利用時の日、エリアコード
利用空間調査情報 (各エンティティーのIDリスト)
配信サービス内で購入者が所持するディスカウント情報 (マイレージ/割り引きクーポン)
コンテンツ単位の購入、利用における購入者、利用者 が所持するディスカウント情報 (マイレージ/割り引きクーポン)
Usage Control 再生課金 Pay-Per-Use 上限回数(-->Sell Through) 1回/2回/....n回の価格

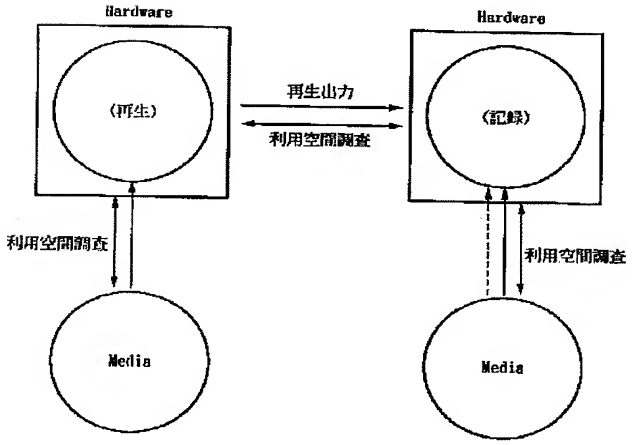
【図１６】



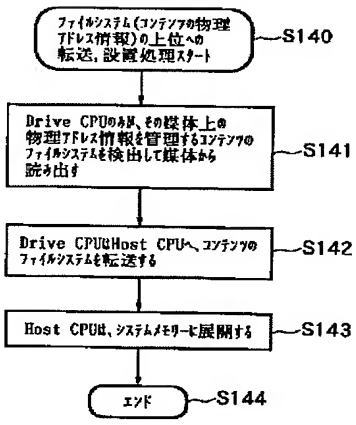
【図８】


System Memory
FS of CF
512
構成されているメディアが
AVCSD系メディアである
Host CPU
510
EMD/SCMS系
フォーマット識別ID
Flash-EEPROM
FS of CF
514
KF1-UCP
KF2-UCP
KF3-UCP
XFn-UCP
KF1-UCS
KF2-UCS
タスク依頼 600
I/O Read/Write
内部割り込み
(ファンクションコール)
SAM
Host CPU Bus
516
専用バス
I/O Read/Write
タスク結果通知
(認証成功/失敗)
(割り込み←
データポーリング→)
外部割り込み(非同期イベント)
Drive CPU
520
公開鍵暗号方式をベース
とした相互認証
Disc Loading
割り込みタイプ xxx H
Switch
526
EMD/SCMS系判別
割り込みタイプxxxH
Media SAM ID
522
(真性)乱数生成:相互認証開始セッション
716
610
Media-SAM
Media Unique ID
Storage Key
FS of XF
KF1～KFn
524
検出器
Revocation List
FS of CF
CF1～CFn
712
710
AVCSD/SCMS系判別用
ユーザの選択により、マニュアルで切り換えられる
414

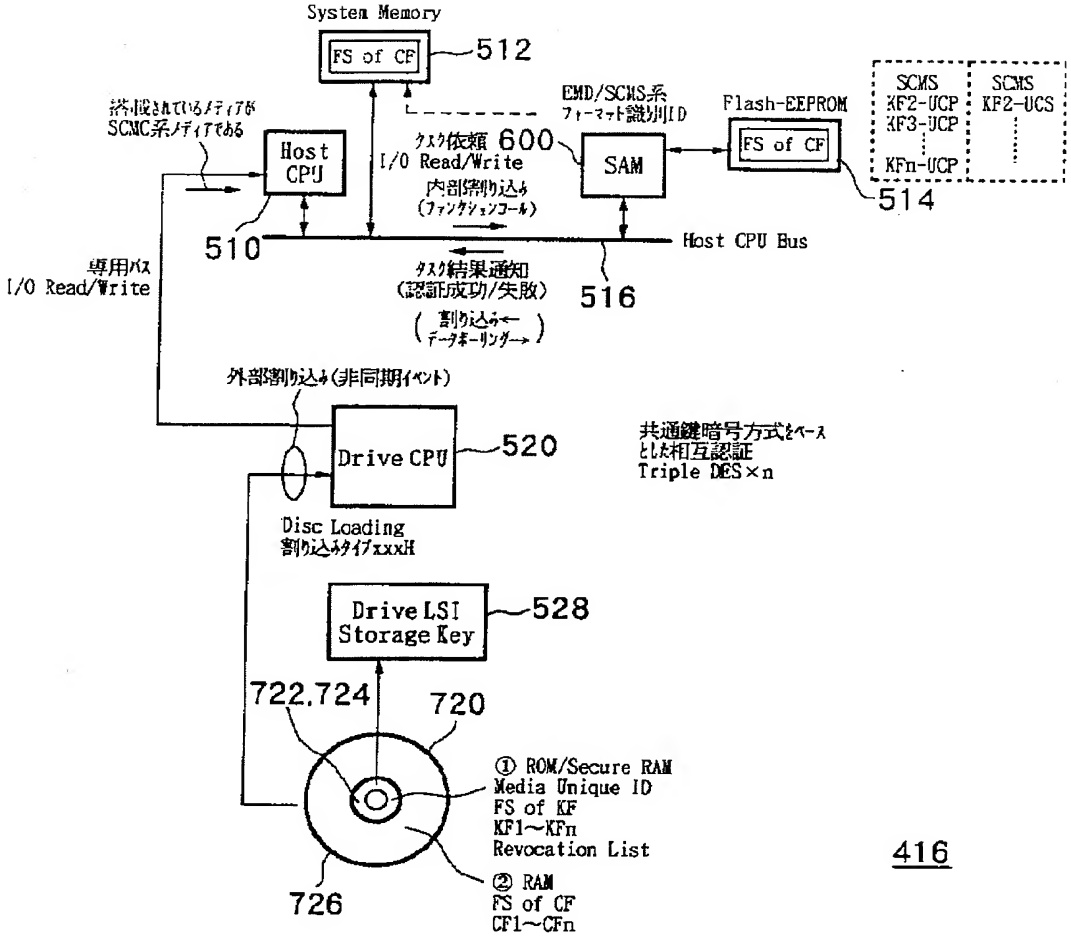
【図１７】


Hardware
(再生)
再生出力
利用空間調査
Hardware
(記録)
利用空間調査
利用空間調査
Media
Media

【図２７】


ファイルシステム(コンテンツの物理アドレス情報)の上位への転送,設置処理スタート
S140
Drive CPUのみM、その媒体上の物理アドレス情報を管理するコンテンツのファイルシステムを検出して媒体から読み出す
S141
Drive CPU&Host CPUへ、コンテンツのファイルシステムを転送する
S142
Host CPUは、システムメモリーに展開する
S143
エンド
S144

【図９】

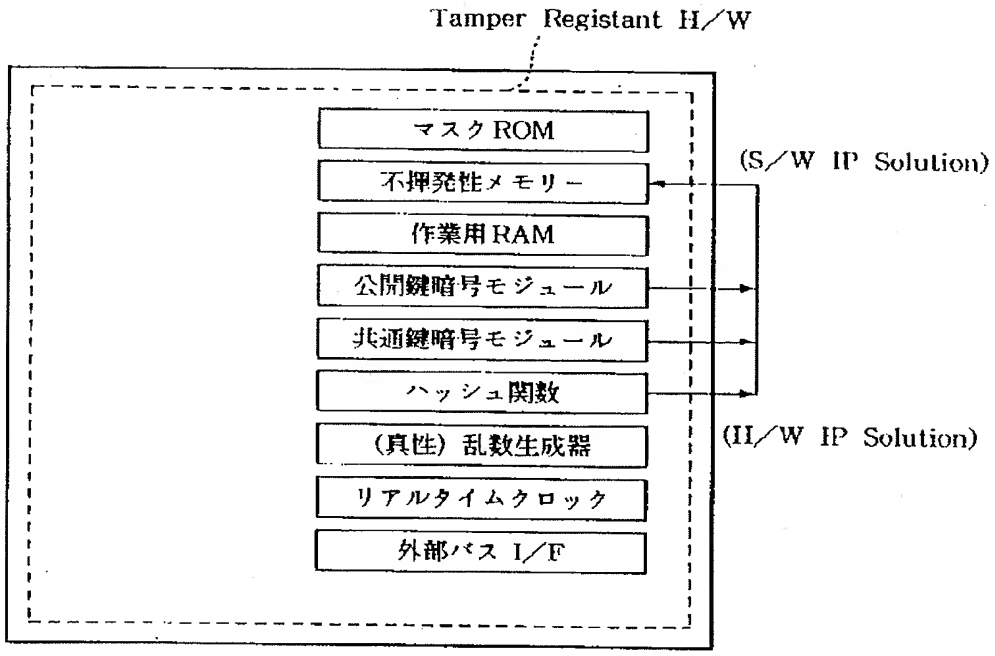


【図１９】

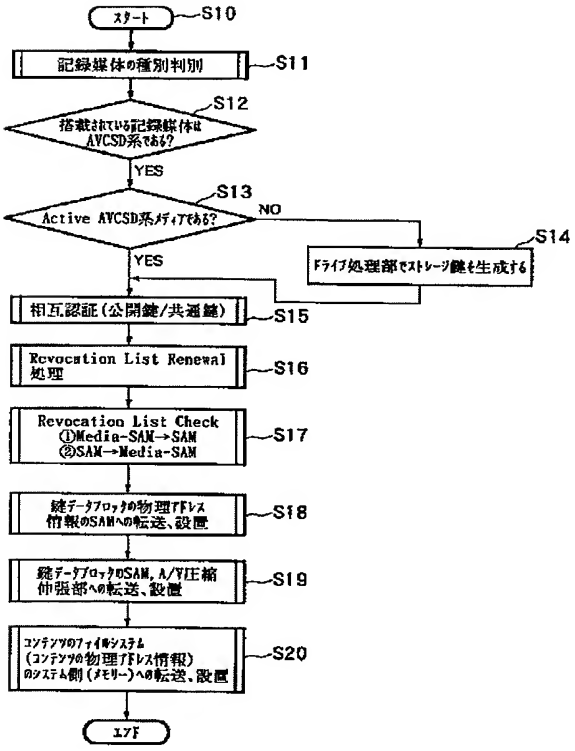
ホームネットワークでの利用空間調査（1対同時多）

コンテンツUCP	再生機器	再生メディア	記録機器1	記録メディア1	記録機器2	記録メディア2-1	記録メディア2-2	記録メディア2-3

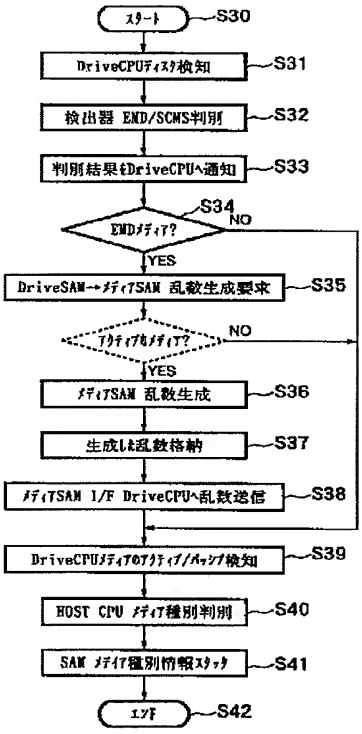
【図１１】


Tamper Registant H／W
マスクROM
不揮発性メモリー
作業用RAM
公開鍵暗号モジュール
共通鍵暗号モジュール
ハッシュ関数
(真性) 乱数生成器
リアルタイムクロック
外部バス I／F
(S／W IP Solution)
(H／W IP Solution)

【図２０】


スタート
S10
記録媒体の種別判別
S11
搭載されている記録媒体はAVCSD系である?
S12
YES
Active AVCSD系メディアである?
S13
NO
S14
Fライブ処理部でストレージ鍵を生成する
YES
相互認証(公開鍵/共通鍵)
S15
Revocation List Renewal処理
S16
Revocation List Check
①Media-SAM→SAM
②SAM→Media-SAM
S17
鍵データブロックの物理アドレス情報のSAMへの転送、設置
S18
鍵データブロックのSAM, A/V圧縮伸張部への転送、設置
S19
コンテンツのファイルシステム(コンテンツの物理アドレス情報)のシステム側(メモリー)への転送、設置
S20
エンド

【図２１】


スタート
S30
DriveCPUディスク検知
S31
検出器 END/SCMS判別
S32
判別結果をDriveCPUへ通知
S33
END メディア?
S34
NO
YES
DriveSAM→メディアSAM 乱数生成要求
S35
アクティブなメディア?
NO
YES
メディアSAM 乱数生成
S36
生成した乱数格納
S37
メディアSAM I/F DriveCPUへ乱数送信
S38
DriveCPUメディアのアクティブ/パッシブ検知
S39
HOST CPU メディア種別判別
S40
SAM メディア種別情報スタック
S41
エンド
S42

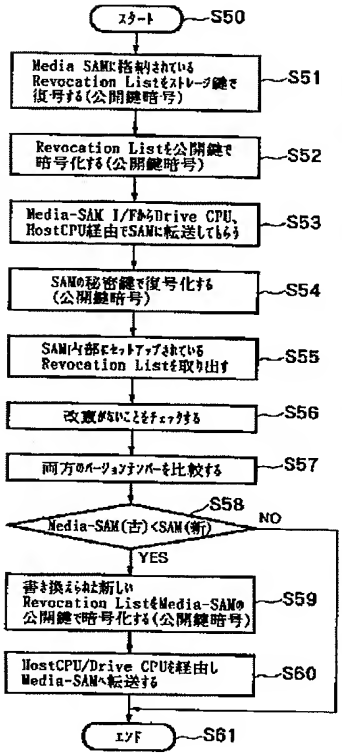
【図１８】

利用空間テーブル

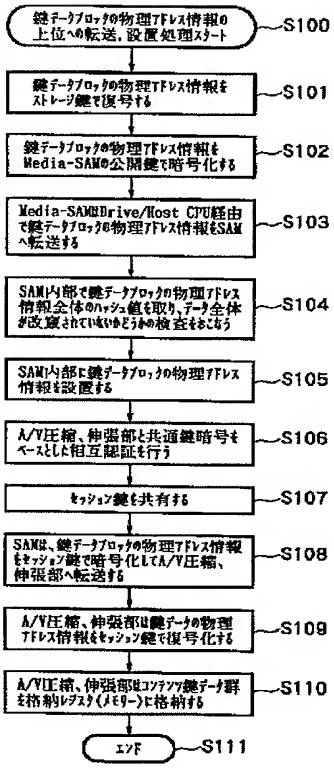
コンテンツ　使用許諾条件　UCP/UCS, U-TOC	
EMD系コンテンツ/SCMS系コンテンツ U-TOC コンテンツの権利処理 UCP 信号諸元、圧縮コーデック方式 UCP 推奨するモニタの表示機能 UCP 個人情報(購入者情報) UCS 権利処理(利益分配)データ UCS　関連エンティティ ID Content Provider ID Service Provider ID 第3信頼機関ID	
再生機器　HNG-ID	再生機器に搭載されているメディア
EMD系機器/SCMS系機器 ビットストリームレコーダor/not 信号諸元 圧縮コーデック方式 接続するモニタの表示能力 フォーマット変換機能 有/無 (有の場合、どのような変換 機能を保持しているか?) eg. 1bit, 1.2882M→16bit, 44.1K 権利処理(利益分配)用データ 関連エンティティ ID 機器ID 機器開発メーカID その他利益分配したい関連 エンティティ ID 登録している第3信頼機関ID	EMD系メディア/SCMS系メディア メディアタイプ　①メディアの種別 ②ROM/RAM 権利処理(利益分配)用データ 関連エンティティ ID 媒体ID 媒体開発メーカID その他利益分配したい関連 エンティティ ID 登録している第3信頼機関ID

記録機器　HNG-ID	記録機器に搭載されているメディア
EMD系機器/SCMS系機器 ビットストリームレコーダor/not 信号諸元 圧縮コーデック方式 接続するモニタの表示能力 諸元変換機能 有/無 (有の場合、どのような変換 機能を保持しているか?) eg. 1bit, 1.2882M→16bit, 44.1K 権利処理(利益分配)用データ 関連エンティティ ID 機器ID 機器開発メーカID その他利益分配したい関連 エンティティ ID 登録している第3信頼機関ID	EMD系メディア/SCMS系メディア メディアタイプ　①メディアの種別 ②ROM/RAM 権利処理(利益分配)用データ 関連エンティティ ID 媒体ID 媒体開発メーカID その他利益分配したい関連 エンティティ ID 登録している第3信頼機関ID

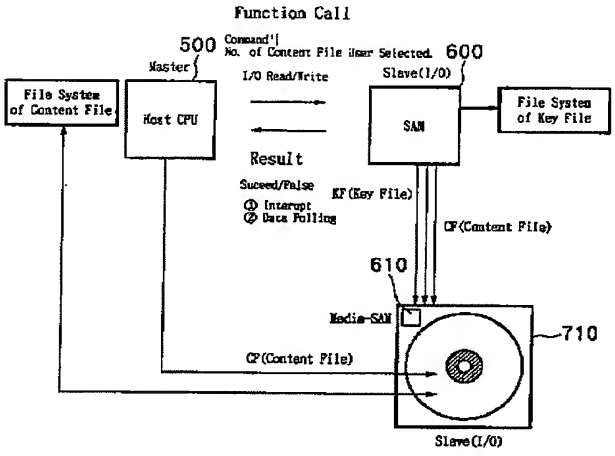
【図２３】



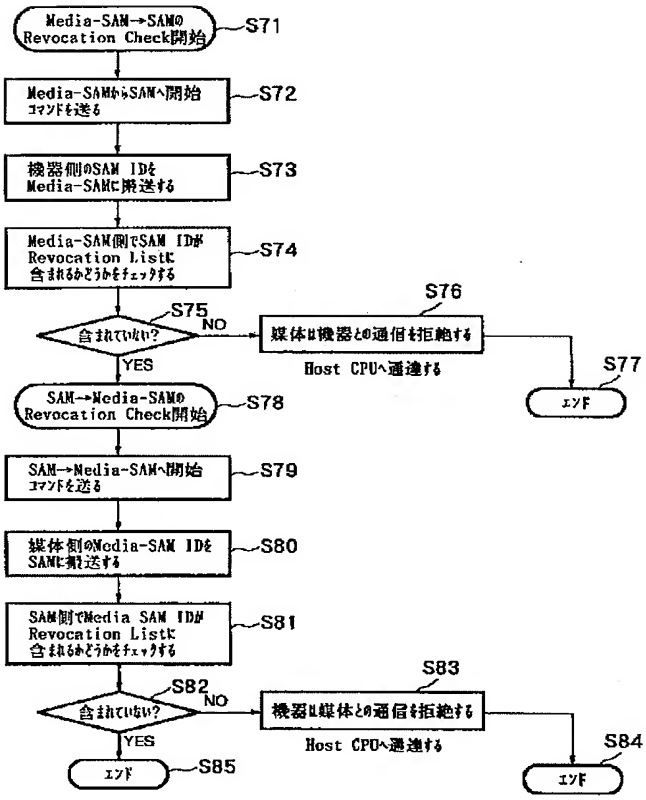
【図２５】



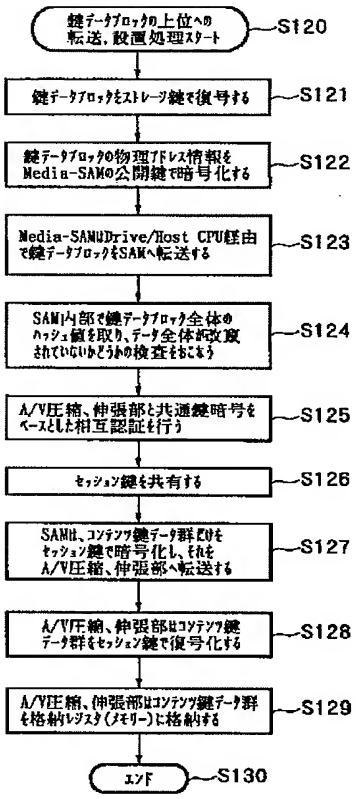
【図２８】



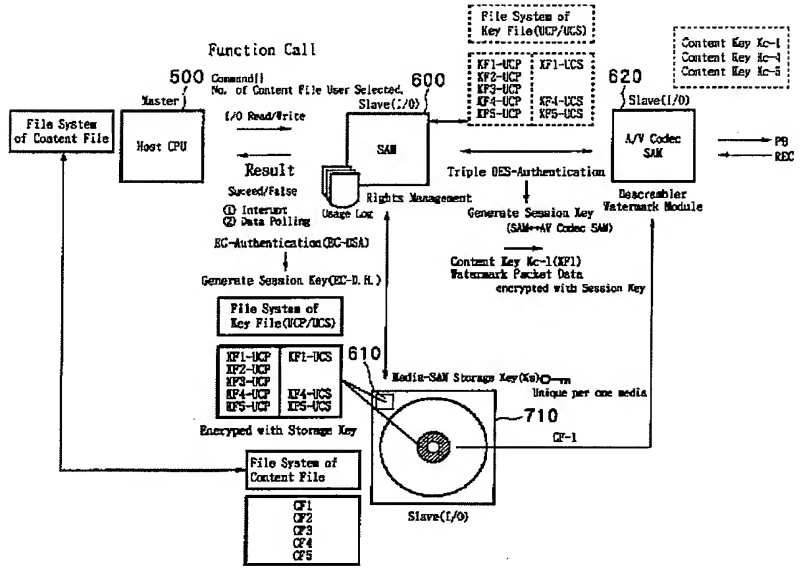
【図２４】



【図２６】



【図２９】



【図４３】

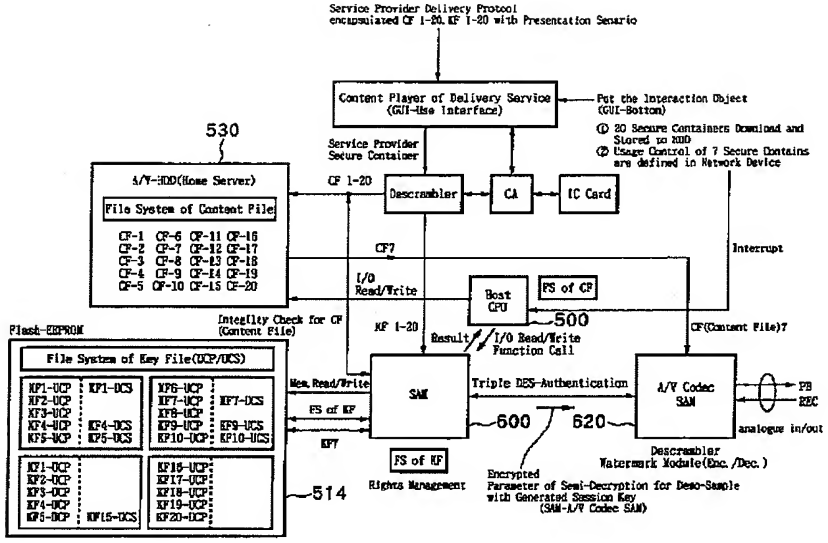
Content ID
User_ID
Home Network Group ID
SAM_ID
Purchase／Usage mode : Sell Through
Price Tag 3

area-code
discount information

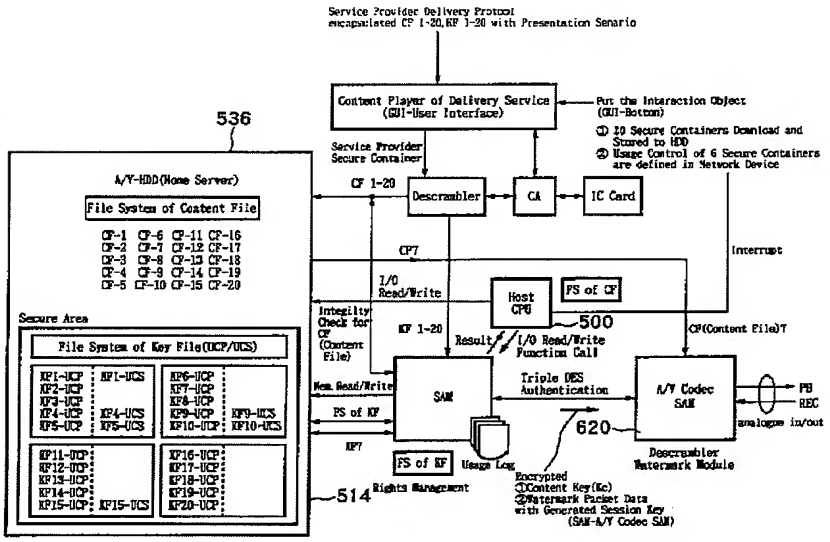
Content Provider ID	xxx
Service Provider ID	xxx
E.M_Place ID	xxx
H/W Provider ID	xxx
Media Provider ID	xxx
Component Provider ID	xxx
Licence Holders ID	xxx
Each Entities ID	xxx
ESC ID	xxx
User ID	xxx

1bit,2.8224MHz→
16bit,44.1KHz,ATRAC2
SACD→MD

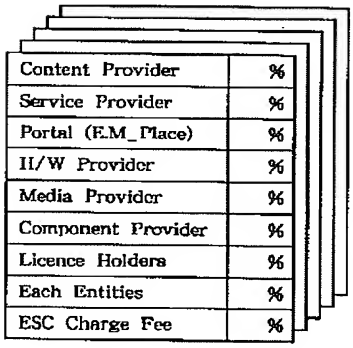
【図３０】



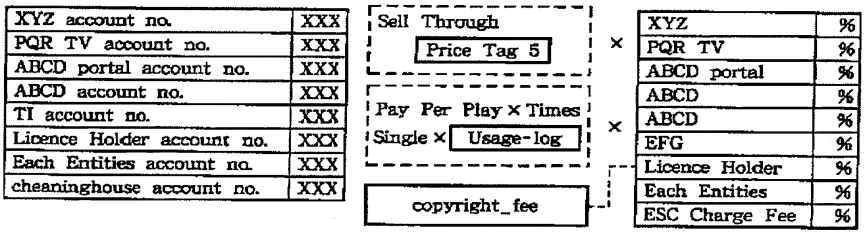
【図３１】



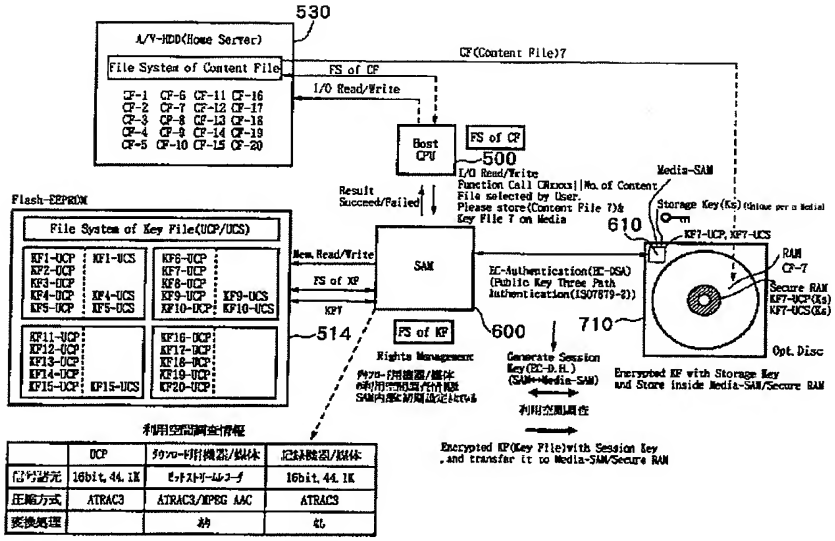
【図４５】



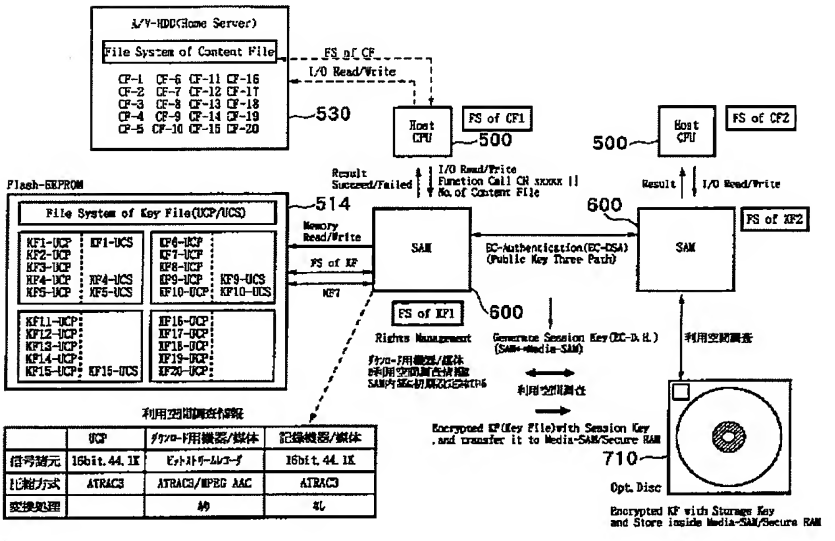
【図４６】



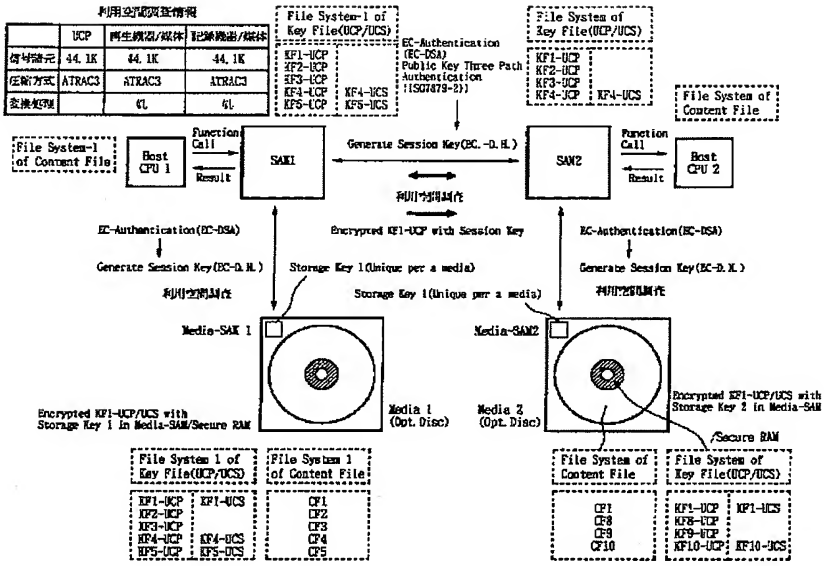
【図３２】


530
A/V-HDD(Home Server)
File System of Content File
CF-1 CF-6 CF-11 CF-16
CF-2 CF-7 CF-12 CF-17
CF-3 CF-8 CF-13 CF-18
CF-4 CF-9 CF-14 CF-19
CF-5 CF-10 CF-15 CF-20
FS of CF
I/O Read/Write
CF(Content File)7
Host CPU
FS of CF
500
I/O Read/Write
Function Call CHxxxx||No. of Content
File selected by User.
Please store(Content File 7)&
Key File 7 on Media
Result
Succeed/Failed
Media-SAM
Storage Key(Ks)
610
KF7-UCP, KF7-UCS
RAM
CF-7
Secure RAM
KF7-UCP(Ks)
KF7-UCS(Ks)
Opt. Disc
Flash-EEPROM
File System of Key File(UCP/UCS)
KF1-UCP KF2-UCP KF3-UCP KF4-UCP KF5-UCP
KF1-UCS KF4-UCS KF5-UCS
KF6-UCP KF7-UCP KF8-UCP KF9-UCP KF10-UCP
KF9-UCS KF10-UCS
KF11-UCP KF12-UCP KF13-UCP KF14-UCP KF15-UCP
KF15-UCS
KF16-UCP KF17-UCP KF18-UCP KF19-UCP KF20-UCP
Mem. Read/Write
FS of KF
KF7
514
SAM
EC-Authentication(EC-DSA)
(Public Key Three Path
Authentication(ISO7816-3))
FS of KF
600
710
Rights Management
Generate Session
Key(EC-D.H.)
(SAM+-Media-SAM)
利用空間調査
Encrypted KF with Storage Key
and Store inside Media-SAM/Secure RAM
Encrypted KF(Key File)with Session Key
, and transfer it to Media-SAM/Secure RAM
利用空間調査情報
UCP
記録機器/媒体
信号諸元
16bit, 44.1K
圧縮方式
ATRAC3
変換処理
なし

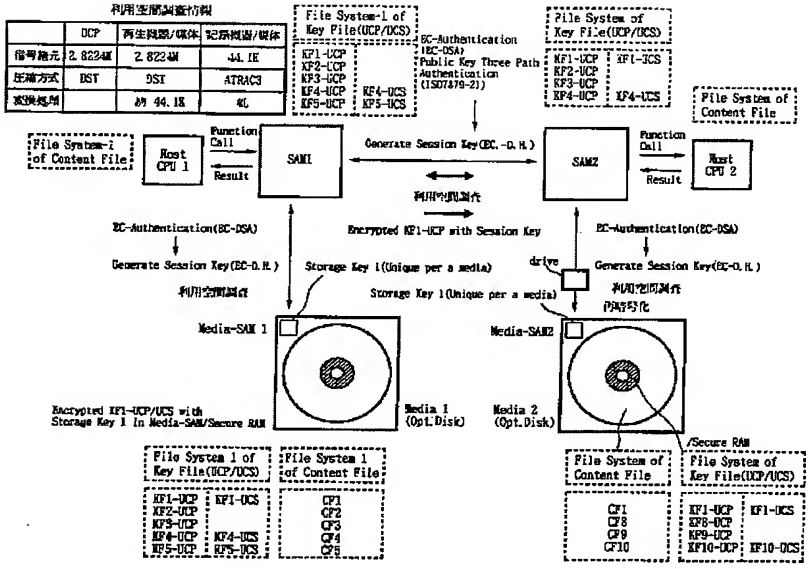
【図３３】


A/V-HDD(Home Server)
File System of Content File
CF-1 CF-6 CF-11 CF-16
CF-2 CF-7 CF-12 CF-17
CF-3 CF-8 CF-13 CF-18
CF-4 CF-9 CF-14 CF-19
CF-5 CF-10 CF-15 CF-20
FS of CF
I/O Read/Write
530
Host CPU
FS of CF1
500
500
Host CPU
FS of CF2
Result
Succeed/Failed
I/O Read/Write
Function Call CH xxxx ||
No. of Content File
Result
I/O Read/Write
Flash-EEPROM
File System of Key File(UCP/UCS)
514
600
FS of KF2
KF1-UCP KF2-UCP KF3-UCP KF4-UCP KF5-UCP
KF1-UCS KF4-UCS KF5-UCS
KF6-UCP KF7-UCP KF8-UCP KF9-UCP KF10-UCP
KF9-UCS KF10-UCS
KF11-UCP KF12-UCP KF13-UCP KF14-UCP KF15-UCP
KF15-UCS
KF16-UCP KF17-UCP KF18-UCP KF19-UCP KF20-UCP
Memory
Read/Write
FS of KF
KF7
SAM
EC-Authentication(EC-DSA)
(Public Key Three Path)
SAM
FS of KF1
600
Rights Management
Generate Session Key(EC-D.H.)
(SAM+-Media-SAM)
利用空間調査
利用空間調査
Encrypted KF(Key File)with Session Key
, and transfer it to Media-SAM/Secure RAM
710
Opt. Disc
Encrypted KF with Storage Key
and Store inside Media-SAM/Secure RAM
利用空間調査情報
UCP
記録機器/媒体
信号諸元
16bit, 44.1K
圧縮方式
ATRAC3
変換処理
なし

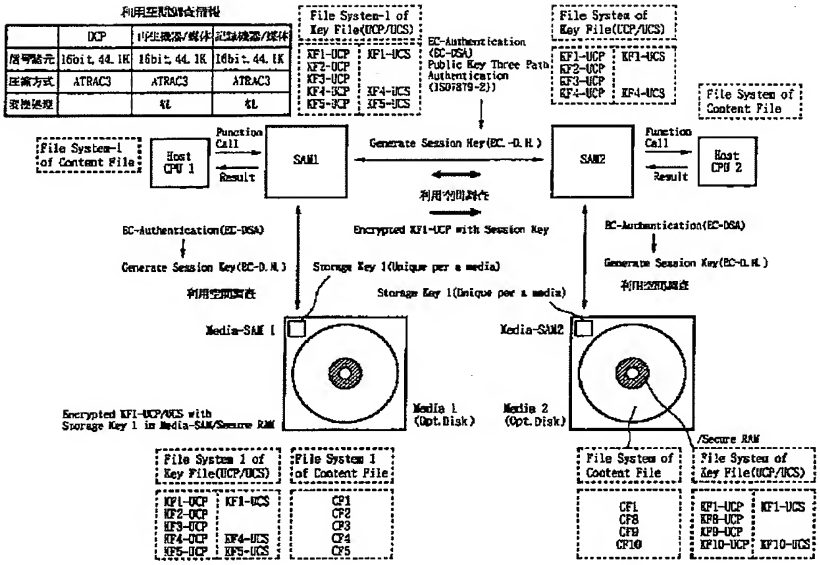
【図３４】


利用空間関連情報
UCP
再生機器/媒体
記録機器/媒体
信号諸元
44.1K
44.1K
44.1K
圧縮方式
ATRAC3
ATRAC3
ATRAC3
変換処理
なし
なし
File System-1 of Key File(UCP/UCS)
KF1-UCP
KF2-UCP
KF3-UCP
KF4-UCP
KF5-UCP
KF4-UCS
KF5-UCS
EC-Authentication (EC-DSA) Public Key Three Path Authentication (ISO7879-2))
File System of Key File(UCP/UCS)
KF1-UCP
KF2-UCP
KF3-UCP
KF4-UCP
KF4-UCS
File System of Content File
File System-1 of Content File
Function Call
Result
Host CPU 1
SAM1
Generate Session Key(EC.-D.H.)
SAM2
Host CPU 2
利用空間関連
EC-Authentication(EC-DSA)
Encrypted KF1-UCP with Session Key
Generate Session Key(EC-D.H.)
Storage Key 1(Unique per a media)
Media-SAM 1
Media-SAM2
Encrypted KF1-UCP/UCS with Storage Key 1 in Media-SAM/Secure RAM
Media 1 (Opt. Disc)
Media 2 (Opt. Disc)
Encrypted KF1-UCP/UCS with Storage Key 2 in Media-SAM
/Secure RAM
File System 1 of Key File(UCP/UCS)
File System 1 of Content File
CF1
CF2
CF3
CF4
CF5
File System of Content File
File System of Key File(UCP/UCS)
CF1
CF8
CF9
CF10
KF1-UCP
KF6-UCP
KF9-UCP
KF10-UCP
KF1-UCS
KF10-UCS

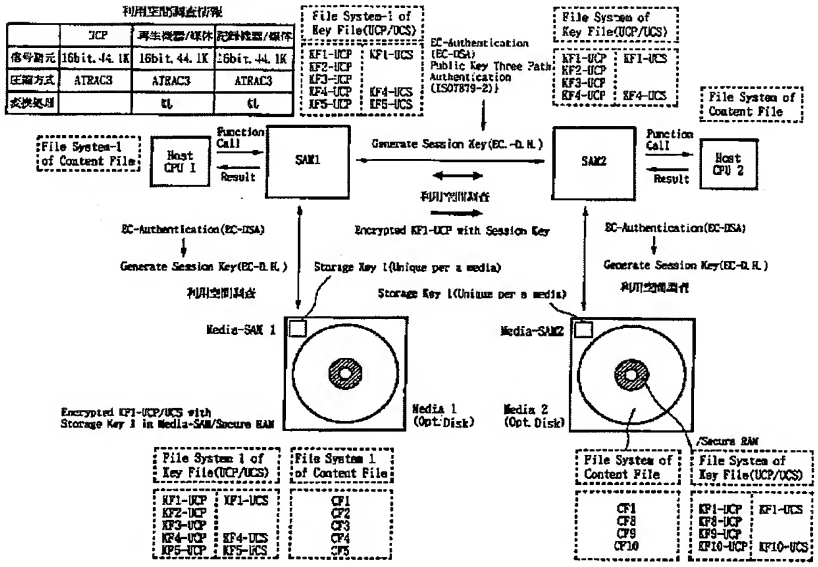
【図３５】


利用空間関連情報
UCP
再生機器/媒体
記録機器/媒体
信号諸元
2.8224M
2.8224M
44.1K
圧縮方式
DST
DST
ATRAC3
変換処理
なし
約 44.1K
なし
File System-1 of Key File(UCP/UCS)
KF1-UCP
KF2-UCP
KF3-UCP
KF4-UCP
KF5-UCP
KF4-UCS
KF5-UCS
EC-Authentication (EC-DSA) Public Key Three Path Authentication (ISO7879-2))
File System of Key File(UCP/UCS)
KF1-UCP
KF2-UCP
KF3-UCP
KF4-UCP
KF1-UCS
KF4-UCS
File System of Content File
File System-1 of Content File
Function Call
Result
Host CPU 1
SAM1
Generate Session Key(EC.-D.H.)
SAM2
Host CPU 2
利用空間関連
EC-Authentication(EC-DSA)
Encrypted KF1-UCP with Session Key
Generate Session Key(EC-D.H.)
Storage Key 1(Unique per a media)
drive
Media-SAM 1
Media-SAM2
Encrypted KF1-UCP/UCS with Storage Key 1 in Media-SAM/Secure RAM
Media 1 (Opt.Disk)
Media 2 (Opt.Disk)
/Secure RAM
File System 1 of Key File(UCP/UCS)
File System 1 of Content File
CF1
CF2
CF3
CF4
CF5
File System of Content File
File System of Key File(UCP/UCS)
CF1
CF8
CF9
CF10
KF1-UCP
KF6-UCP
KF9-UCP
KF10-UCP
KF1-UCS
KF10-UCS

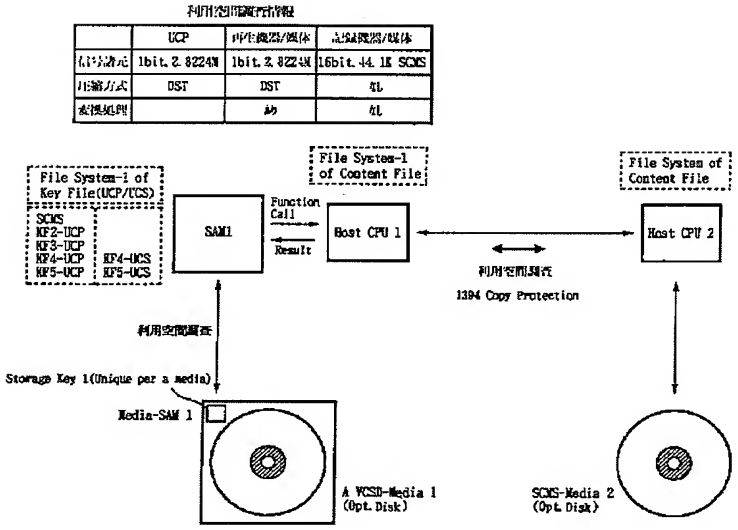
【図３６】


File System-1 of Key File(UCP/UCS)
File System of Key File(UCP/UCS)
EC-Authentication (EC-DSA) Public Key Three Path Authentication (ISO7816-2))
File System of Content File
File System-1 of Content File
Host CPU 1
Function Call
Result
SAM1
Generate Session Key(EC.-D.H.)
SAM2
Host CPU 2
利用空間調査
EC-Authentication(EC-DSA)
Encrypted KF1-UCP with Session Key
Generate Session Key(EC-D.H.)
Storage Key 1(Unique per a media)
Media-SAM 1
Media-SAM2
Encrypted KF1-UCP/UCS with Storage Key 1 in Media-SAM/Secure RAM
Media 1 (Opt.Disk)
Media 2 (Opt.Disk)
/Secure RAM
KF1-UCP
KF2-UCP
KF3-UCP
KF4-UCP
KF5-UCP
KF1-UCS
KF4-UCS
KF5-UCS
CF1
CF2
CF3
CF4
CF5
CF8
CF9
CF10
KF8-UCP
KF9-UCP
KF10-UCP
KF10-UCS

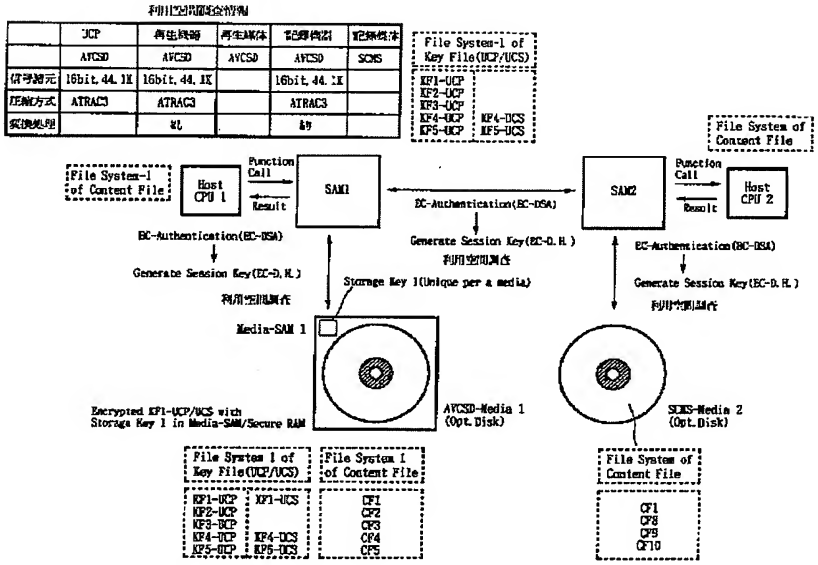
【図３７】


File System-1 of Key File(UCP/UCS)
File System of Key File(UCP/UCS)
EC-Authentication (EC-DSA) Public Key Three Path Authentication (ISO7816-2))
File System of Content File
File System-1 of Content File
Host CPU 1
Function Call
Result
SAM1
Generate Session Key(EC.-D.H.)
SAM2
Host CPU 2
利用空間調査
EC-Authentication(EC-DSA)
Encrypted KF1-UCP with Session Key
Generate Session Key(EC-D.H.)
Storage Key 1(Unique per a media)
Media-SAM 1
Media-SAM2
Encrypted KF1-UCP/UCS with Storage Key 1 in Media-SAM/Secure RAM
Media 1 (Opt.Disk)
Media 2 (Opt.Disk)
/Secure RAM
KF1-UCP
KF2-UCP
KF3-UCP
KF4-UCP
KF5-UCP
KF1-UCS
KF4-UCS
KF5-UCS
CF1
CF2
CF3
CF4
CF5
CF8
CF9
CF10
KF8-UCP
KF9-UCP
KF10-UCP
KF10-UCS

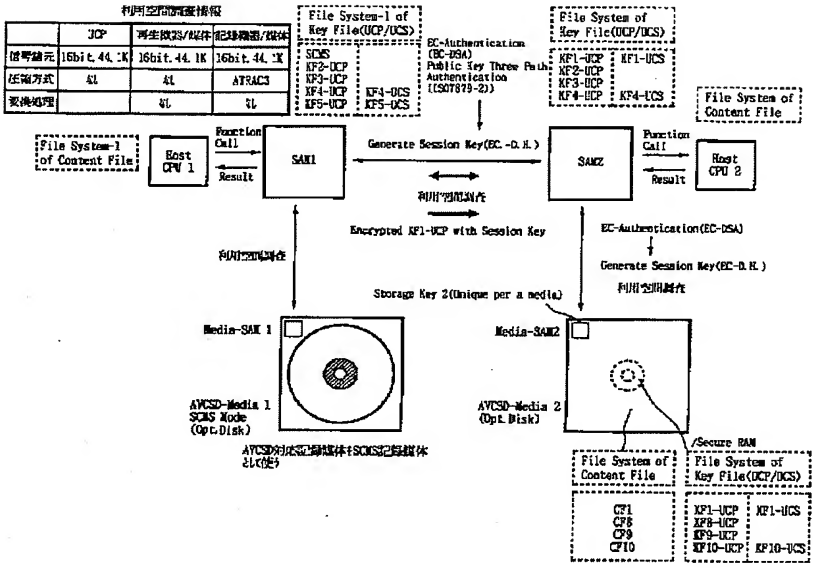
【図３８】


利用空間調査情報
UCP
再生機器/媒体
記録機器/媒体
信号単元
1bit, 2.8224M
1bit, 2.8224M
16bit, 44.1K SCMS
圧縮方式
DST
DST
なし
変換処理
あり
なし
File System-1 of Key File(UCP/UCS)
SCMS
KF2-UCP
KF3-UCP
KF4-UCP
KF5-UCP
KF4-UCS
KF5-UCS
SAM1
Function Call
Result
File System-1 of Content File
Host CPU 1
File System of Content File
Host CPU 2
利用空間調査
1394 Copy Protection
利用空間調査
Storage Key 1(Unique per a media)
Media-SAM 1
A VCSD-Media 1 (Opt. Disk)
SCMS-Media 2 (Opt. Disk)

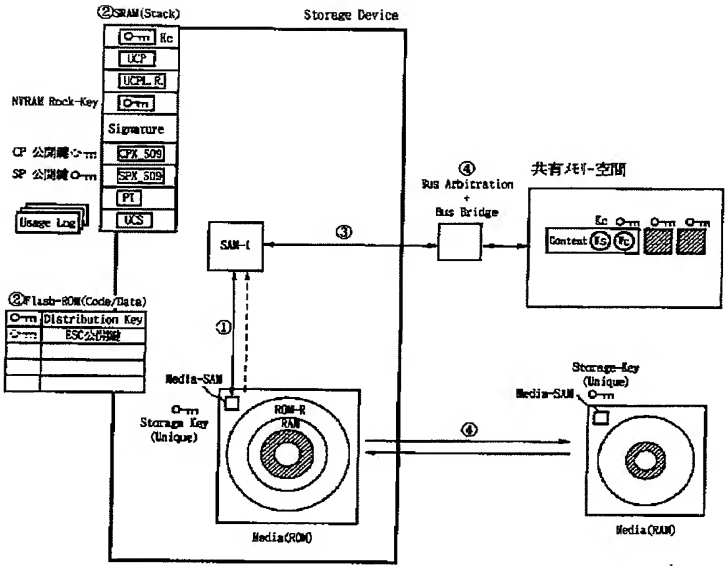
【図３９】


利用空間調査情報
UCP
再生機器
再生媒体
記録機器
記録媒体
AVCSD
AVCSD
AVCSD
AVCSD
SCMS
信号単元
16bit, 44.1K
16bit, 44.1K
16bit, 44.1K
圧縮方式
ATRAC3
ATRAC3
ATRAC3
変換処理
なし
あり
File System-1 of Key File(UCP/UCS)
KF1-UCP
KF2-UCP
KF3-UCP
KF4-UCP
KF5-UCP
KF4-UCS
KF5-UCS
File System of Content File
File System-1 of Content File
Host CPU 1
Function Call
Result
SAM1
EC-Authentication(EC-DSA)
Generate Session Key(EC-D.H.)
利用空間調査
SAM2
Host CPU 2
Storage Key 1(Unique per a media)
Media-SAM 1
Encrypted KF1-UCP/UCS with Storage Key 1 in Media-SAM/Secure RAM
AVCSD-Media 1 (Opt. Disk)
SCMS-Media 2 (Opt. Disk)
File System 1 of Key File(UCP/UCS)
KF1-UCS
File System 1 of Content File
CF1
CF2
CF3
CF4
CF5
CF9
CF10

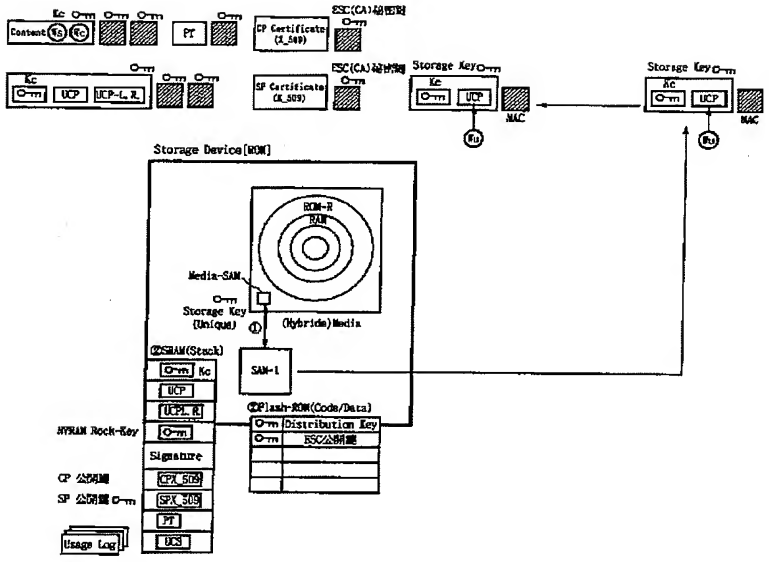
【図４０】


File System-1 of Key File(UCP/UCS)
File System of Key File(UCP/UCS)
EC-Authentication (EC-DSA) Public Key Three Path Authentication (ISO7816-2))
File System of Content File
File System-1 of Content File
Host CPU 1
Function Call
Result
SAM1
Generate Session Key(EC.-D.H.)
SAM2
Host CPU 2
Encrypted KF1-UCP with Session Key
EC-Authentication(EC-DSA)
Generate Session Key(EC-D.H.)
Storage Key 2(Unique per a media)
Media-SAM 1
Media-SAM2
AVCSD-Media 1 SCSAS Mode (Opt.Disk)
AVCSD-Media 2 (Opt.Disk)
/Secure RAM
File System of Content File
File System of Key File(UCP/UCS)

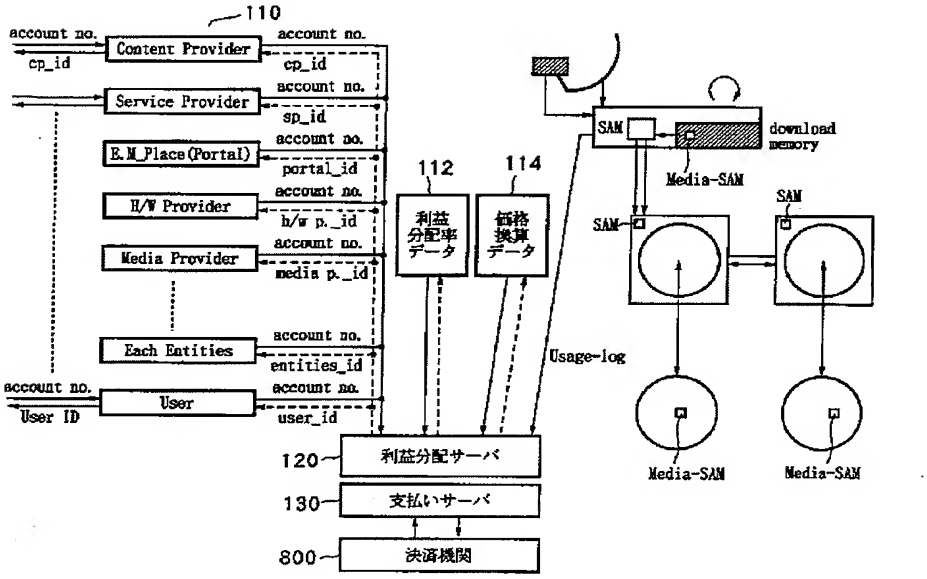
【図４１】


②SRAM(Stack)
Storage Device
Kc
UCP
UCPL.R
NFRAM Rock-Key
Signature
CP 公開鍵
SP 公開鍵
CPX.509
SPX.509
PI
Usage Log
UCS
②Flash-ROM(Code/Data)
Distribution Key
ESC公開鍵
SAM-1
③
④
Bus Arbitration + Bus Bridge
共有メモリ空間
Content
Media-SAM
Storage Key (Unique)
ROM-R RAM
Media(ROM)
Storage-Key (Unique)
Media-SAM
Media(RAM)

【図４２】


Storage Device[ROM]
Media-SAM
Storage Key
(Unique)
(Hybride)Media
SAM-1
Distribution Key
Signature
Usage Log

【図４４】


110
Content Provider
Service Provider
E.M_Place(Portal)
H/W Provider
Media Provider
Each Entities
User
account no.
cp_id
sp_id
portal_id
h/w p._id
media p._id
entities_id
user_id
User ID
112
利益分配率データ
114
価格換算データ
SAM
download memory
Media-SAM
Usage-log
120
利益分配サーバ
130
支払いサーバ
800
決済機関